All Versions
Users Manual

Version 5.0.1

Table of Contents

Welcome to F-Response 4
Terminology 4
Target....4
Initiator....4
Supported Platforms....5
Prerequisites....6
F-Response License FOB....7
Getting started with F-Response 9
Enterprise Edition 9
Consultant + Covert Edition 10
Consultant Edition....11
Field Kit Edition 12
Licensing F-Response 13
Using the F-Response License Manager Software (CE and EE Only) 13
Installing and starting the F-Response License Manager....15
F-Response Cloud Connector 17
Using the F-Response Cloud Connector (TAC,CE,CE+C, and EE) 17
Configuring Cloud Credentials....18
Scanning for Cloud Storage Targets 35
Connecting to Cloud Storage Targets 36
Disconnecting from Cloud Storage Targets 37
F-Response Database Object Connector 38
Using the F-Response Database Object Connector (TAC,CE,CE+C, and EE) 38
Configuring Database Server Credentials....39
Scanning for Database Object Targets 40
Connecting to Database Object Targets 41
Disconnecting from Database Object Targets 42
F-Response Email Connector....43
Using the F-Response Email Connector (TAC,CE,CE+C, and EE) 43
Configuring Email Credentials 44
Scanning for Email Account Targets....45
Connecting to Email Account Targets 46
Disconnecting from Email Account Targets 47
F-Response Enterprise....49
Enterprise Edition – Overview of the F-Response Enterprise Management Console (FEMC)....49
Enterprise Edition – Configuring the FEMC Deployment Options....52
Enterprise Edition – Configuring the FEMC Credentials 54
Enterprise Edition – Scanning 56
Enterprise Edition – Deploying and Managing F-Response using the FEMC (All Supported Platforms) 58
Enterprise Edition – Using F-Response Enterprise Edition for Windows (Deployment without the FEMC)....67
F-Response Consultant + Covert Edition....68
Consultant + Covert Edition – Overview....68
F-Response Consultant Edition....69
Consultant Edition – Overview of the F-Response Consultant Connector....69
Consultant Edition – Configuring the FCC Console (Quick Configure)....71
Consultant Edition – Configuring the FCC Console (Create AutoConfigure)....72
Consultant Edition – Using F-Response Consultant Edition for Windows 74

Consultant Edition – Using F-Response Consultant Edition for Unix based Targets 79
F-Response command line help on analyst machine 79
Consultant Edition – Using the F-Response Consultant Connector 81
F-Response Accelerator (Consultant and Enterprise Only) 85
Field Kit Edition 86
F-Response Field Kit Edition – Using F-Response Field Kit Edition for Windows 86
F-Response Field Kit Edition – Using F-Response Field Kit Edition for Unix (Linux, Apple OS X) 88
F-Response Field Kit Edition – Connecting to an F-Response Target 89
F-Response Field Kit Edition – Disconnecting from an F-Response Target 95
F-Response Flexdisk™ 97
What is a F-Response Flexdisk™? 97
How do I access and use a F-Response Flexdisk™? 97
Frequently Asked Questions 98
Support 101
Mission Guides 102
Software Revision History 103
Appendix A – Overview of the F-Response Enterprise Edition Windows Command Line Interface 113
Appendix B – Overview of the F-Response Enterprise Edition Unix Command Line Interface 115
Appendix C – Overview of the F-Response Consultant User Interface 117
Appendix D – Overview of the F-Response Field Kit User Interface 119
Appendix E – Understanding Unix Credentials 121
Appendix F – Software Requirements on the Target Computer 124
Appendix G – F-Response Target Naming Convention 125
Appendix H -- Icon Legend 126
Appendix I – Master Software License Agreement 128
Appendix J – Renewing F-Response Dongle License 132
Updating the F-Response Dongle (FK,CE,CE+C,EE) 132
Purpose 132
What You Need 132
Appendix K – Legal Notices 133
Legal Notice 133
Trademarks 133
Statement of Rights 133
Disclaimer 133
Patents 133

Welcome to F-Response

Thank you for purchasing F-Response. You have now extended the capabilities of your existing arsenal of tools to enable them to work over an IP network. F-Response accomplishes this through the use of a patented process (US 7,899,882 US 8,171,108 and patents pending); a part of which includes leveraging the Internet Small Computer Systems Interface (iSCSI) protocol standard as defined in RFC 3720 (http://www.ietf.org/rfc/rfc3720.txt).

Terminology

The iSCSI terms "Target" and "Initiator" are used throughout this manual. The choice of "initiator" and "target" verbiage in the iSCSI definitions may prove confusing to forensics practitioners because "target" carries a different definition in the field of computer forensics versus iSCSI. In computer forensics, the system to be analyzed is generally referred to as the "subject" system, whereas the system to which forensically sound data is collected is generally referred to as the "target" system. In this manual, the forensic "subject" is an iSCSI "target", i.e. F-Response Target code is executed on the machine to be analyzed. For this reason, we want to make clear that the use of the word "target" in this manual refers to the iSCSI definition, and not the forensics definition. The definitions for Target and Initiator used in this manual are as follows:

Target

F-Response Target code is to be executed on the machine(s) to be analyzed. All references to "target" in this manual refer to the machine(s) being analyzed using F-Response target code.

Initiator

An iSCSI "initiator" is used to establish network connections to machines running F-Response Target code. iSCSI initiator software must be installed on the machine from which analysis is to be conducted over the network. F-Response Target code has been tested with Microsoft iSCSI Initiator 2.0 software, included by default with newer Windows operating systems, and freely available for download from the Microsoft web site.

Supported Platforms

The F-Response stand alone executable is capable of providing remote forensically sound read only physical hard drive connectivity on the following platforms:

Platforms supported by all versions of F-Response (Field Kit, Consultant, Consultant + Covert, & Enterprise)

- Windows 2000 (Professional, Server, Advanced Server)
- Windows XP (Home, Professional, Professional 64bit)
- Windows 2003
- Windows Vista (32 & 64bit)
- Windows 2008 (32 & 64bit)
- Windows 7 (32bit & 64bit)
- Windows 8 (32bit & 64bit)
- Windows 2012 (64bit)
- Linux (Glibc 2.3.5+)[1]
- Apple OS X (10.3, 10.4, 10.5, 10.6, 10.7, 10.8 Intel[2] Only)

Additional Platforms supported by F-Response Consultant, Consultant + Covert, and Enterprise only

- Apple OS X (10.3, 10.4, 10.5, 10.6, 10.7, 10.8 Universal Binary)
- Sun Solaris (8, 9, 10) on SPARC
- OpenSolaris, Oracle Solaris 11 on Intel
- IBM AIX (5.1, 5.2, 5.3, 6.1, 7) on Power
- HP_UX11iv2 and HP_UX11iv3 on Itanium
- FreeBSD (7,8) on Intel i386,x64
- SCO OpenServer 6 and Unixware 7 on Intel i386
- Google Android (ARM) (Native Code)
- Netgear ReadyNAS (SPARC)

F-Response Flexdisk™ Supported[3] Platforms (Consultant, Consultant + Covert, and Enterprise)

- Windows 2000 (Professional, Server, Advanced Server)
- Windows XP (Home, Professional, Professional 64bit)
- Windows 2003
- Windows Vista (32 & 64bit)
- Windows 2008 (32 & 64bit)
- Windows 7 (32bit & 64bit)
- Windows 8 (32bit & 64bit)
- Windows 2012 (64bit)
- Linux (Glibc 2.3.5+) (32bit and 64bit)
- Apple OS X (10.3, 10.4, 10.5, 10.6, 10.7, 10.8 Universal Binary)

Cloud Storage Environments supported by the F-Response Cloud Connector

- Amazon Web Services Simple Storage Service (S3)

[1] Linux glibc 2.3.5 includes Redhat, Suse, Ubuntu, Fedora, and many other distributions of Linux released during or after 2003.
[2] Intel only for Field Kit, all others are Universal Binary.
[3] Platform support is further restricted to supported filesystems, ext2, ext3, ntfs, fat, hfs, hfs+

- Windows Azure Blob Storage
- Rackspace Cloud Files (US and UK)
- HP Public Cloud
- Any Openstack[4] based Cloud Storage (v1 series)
- Google Drive
- Google Apps for Business Google Drive
- Dropbox
- Microsoft Skydrive

Email Servers supported by the F-Response Email Connector

- Gmail (Google Apps and Gmail)
- Yahoo! Mail
- Most IMAP based Email providers
- Office 365 Exchange Web Services

Database platforms and structures supported by the F-Response Database Object Connector

- Microsoft Sharepoint, Microsoft SQL Server

Prerequisites

In order to use F-Response you will require the following:

1. A valid F-Response License key FOB ("F-Response FOB") which can be purchased from the F-Response Web site www.F-Response.com
2. A copy of the latest F-Response Installation Package for the version selected:
    1. F-Response Enterprise Edition
    2. F-Response Consultant + Covert Edition
    3. F-Response Consultant Edition
    4. F-Response Field Kit Edition
3. Microsoft iSCSI initiator software, included by default with Windows Vista, Server 2008, and Windows 7 operating systems, and freely available for download from the Microsoft web site.

    Note: The Microsoft iSCSI Software Initiator is available as a free download from http://www.microsoft.com/downloads for the following operating systems:

    - Microsoft Windows 2000
    - Microsoft Windows Server 2003
    - Microsoft Windows XP

    This version should not be installed on the following operating systems:

    - Windows Vista
    - Windows Server 2008
    - Windows 7

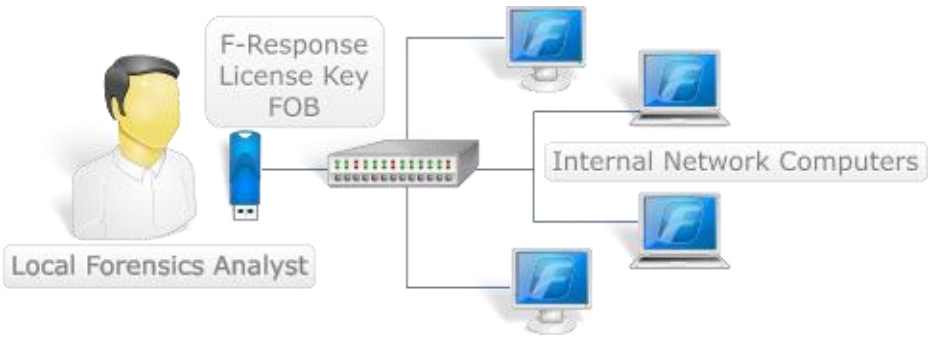
[4] More information on Openstack is available at www.openstack.org

The Microsoft iSCSI Software initiator is integrated into Windows Vista, Windows Server 2008, and Windows 7; therefore there is no need to install this package on those operating system versions.

The Microsoft iSCSI Software initiator configuration utility on Windows Vista and Windows Server 2008 can be accessed from the control panel in classic mode or from administrative tools in Windows Server 2008.

(Source: Microsoft iSCSI Software Initiator 2.x User Guide, Nov 2007)

The diagram below shows a high level architecture for F-Response. The F-Response FOB is located at the analysis machine (Consultant/Enterprise), and the F-Response Target code may be running on any number of corporate networked computers.



F-Response Enterprise High Level Architecture

F-Response License FOB

In order to use the F-Response application you must have a valid F-Response License key FOB ("F-Response FOB"), such as the one shown below:

This key must be inserted into the USB port of *the computer running the F-Response License Manager Server*, the examiner's analysis machine in the case of Enterprise/Consultant Editions, or the target machine if using the Field Kit Edition. Since the F-Response FOB uses the USB Human Interface Device drivers it should be immediately recognized by all supported versions of Microsoft Windows, as shown below.

Operating System response to insertion of the F-Response FOB

Once the F-Response FOB has been inserted and recognized by your analysis machine, you are ready to start the Enterprise Edition of F-Response on the remote workstation and establish an F-Response network connection such that you may begin analysis using your tool(s) of choice.

Getting started with F-Response

Enterprise Edition

If you possess a license for F-Response Enterprise Edition, then you may use your F-Response FOB with any of the F-Response Target code offerings, including the Enterprise Edition ("EE") Target Code, Consultant + Covert Edition ("CE+C") Target Code, Consultant Edition ("CE") Target code, or the Field Kit ("FK") Target code at your discretion. Please refer to the respective user manual sections for instructions on using F-Response in the desired mode.

The Enterprise Edition Installation package installs the following software:

- F-Response License Manager and License Manager Monitor
- F-Response Enterprise Management Console (FEMC)
- F-Response Cloud Connector (FCLDC)
- F-Response Accelerator (FAR)
- F-Response Enterprise COM Object (FEMCCTRL)
- F-Response Enterprise Target Code (All Supported Platforms)
- F-Response Consultant Target Code (All Supported Platforms)
- F-Response Dongle Updater

The default installation is to Program Files -> F-Response. **Do not install this installation package on the machine to be analyzed.**

Consultant + Covert Edition

If you possess a license for F-Response Consultant + Cover Edition, then you may use your F-Response FOB with any of the F-Response Target code offerings, including the Enterprise Edition ("EE") Target Code, Consultant Edition ("CE") Target code, or the Field Kit ("FK") Target code at your discretion. Please refer to the respective user manual sections for instructions on using F-Response in the desired mode.

The Consultant + Covert Edition Installation package installs the following software:

- F-Response License Manager and License Manager Monitor
- F-Response Consultant + Covert Console (FCC+)
- F-Response Cloud Connector (FCLDC)
- F-Response Consultant Connector (FCC)
- F-Response Accelerator (FAR)
- F-Response Consultant COM Object (FCCCTRL)
- F-Response Enterprise Target Code (All Supported Platforms)
- F-Response Consultant Target Code (All Supported Platforms)
- F-Response Dongle Updater

The default installation is to Program Files -> F-Response. **Do not install this installation package on the machine to be analyzed.**

Consultant Edition

If you possess a license for F-Response Consultant (or Enterprise) Edition, then you may use your F-Response FOB with either the Field Kit ("FK") Target code or Consultant Edition ("CE") Target code at your discretion. Please refer to the Field Kit Edition section of the User Manual for instructions on using F-Response in Field Kit mode.

The Consultant Edition Installation package installs the following software:

- F-Response License Manager and License Manager Monitor
- F-Response Consultant Connector (FCC)
- F-Response Accelerator (FAR)
- F-Response Consultant COM Object (FCCCTRL)
- F-Response Consultant Target Code (All Supported Platforms)
- F-Response Dongle Updater

The default installation is to Program Files -> F-Response. **Do not install this installation package on the machine to be analyzed.**

Only the F-Response Consultant Edition Target Code is executed on the machine to be analyzed, and this executable is placed in *Program Files -> F-Response -> F-Response Consultant Edition* upon completion of the package installation.

Field Kit Edition

F-Response Field Kit Edition Target code is a stand alone executable ("exe"). The Field Kit Edition Installation package installs this software ("F-Response Field Kit Edition Target code"), a copy of F-Response Field Kit Edition Target Code which can be copied to any number of computers to be analyzed.

The Field Kit Edition Installation package installs the following software:

- F-Response Field Kit Target Code (All Supported Platforms)
- F-Response Dongle Updater

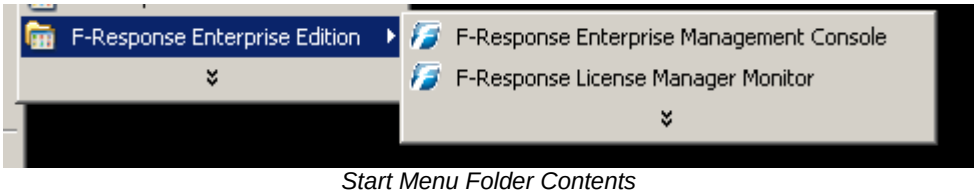
The default installation is to Program Files -> F-Response. **Do not install this installation package on the machine to be analyzed.**

Only the F-Response Field Kit Edition Target Code is executed on the machine to be analyzed, and this executable is placed in *Program Files -> F-Response -> F-Response Field Kit Edition* upon completion of the package installation.

Licensing F-Response

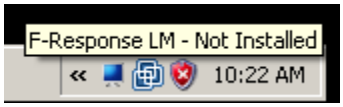
Using the F-Response License Manager Software (CE and EE Only)

In order to validate your license (F-Response FOB) from remote computers running F-Response Enterprise or Consultant Edition target code, you must have your FOB physically connected to your analysis machine and the F-Response License Manager must be started . Execute the F-Response License Manager Monitor.

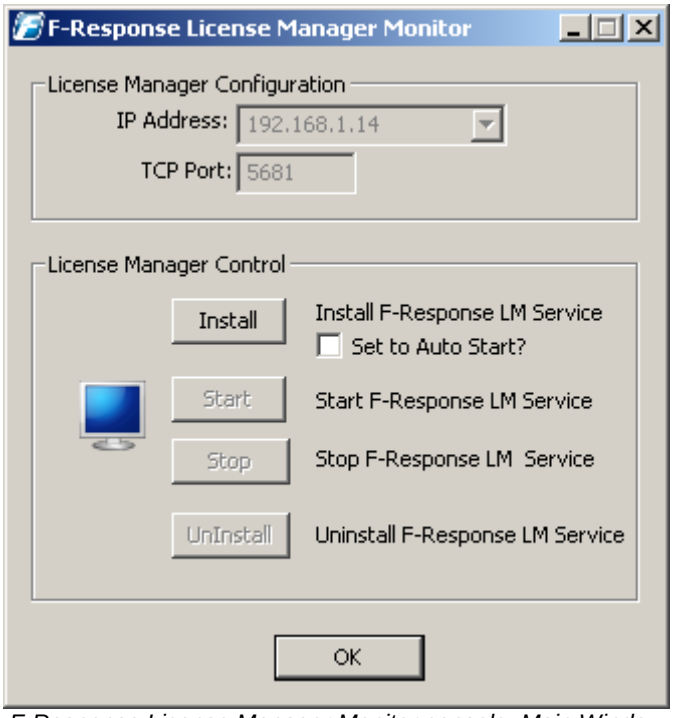


Start Menu Folder Contents

The first time the F-Response License Manager Monitor (F-Response LM) software is executed it will display a System Tray icon indicating the License Manager server is not installed.



System Tray Icon indicating the F-Response LM server is not installed



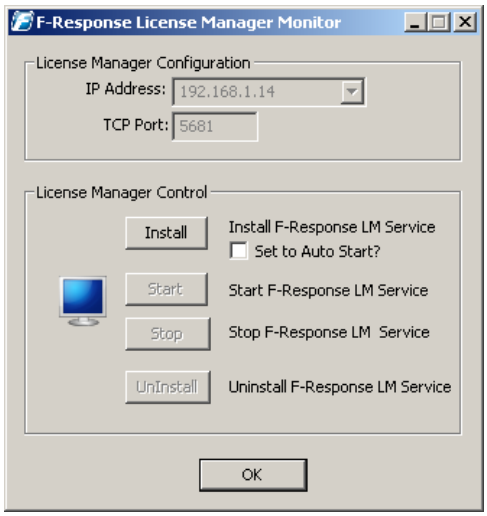
F-Response License Manager Monitor console, Main Window

The representation above shows a running F-Response License Manager Monitor. Details of the information in the Network tab fields are as follows:

- License Manager Configuration
  - IP Address:
    - Local machine IP address currently listening for incoming F-Response Enterprise/Consultant Edition License Validation requests.
  - TCP Port:
    - Local machine TCP port currently listening for incoming F-Response Enterprise/Consultant Edition License Validation requests.
- Operation
  - Install
    - Installs the License Manager Service executable.
  - Start
    - Starts the License Manager Server.
  - Stop
    - Stops the License Manager Server.
  - Uninstall
    - Uninstalls the License Manager Service executable.

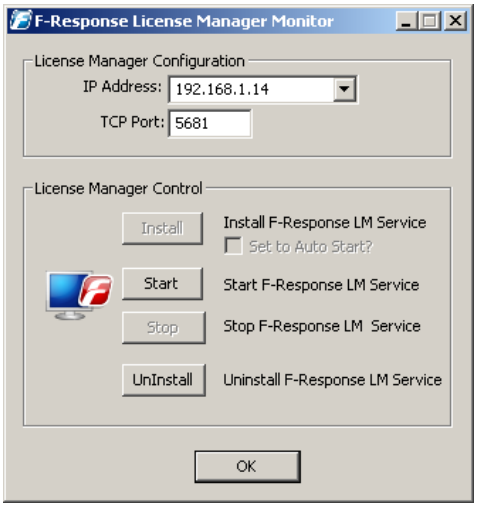
Installing and starting the F-Response License Manager

Before you can begin using F-Response Enterprise and Consultant Edition you must install and start the F-Response License Manager service. Double click on the F-Response License Manager Monitor icon in the System Tray to bring up the License Manager console.



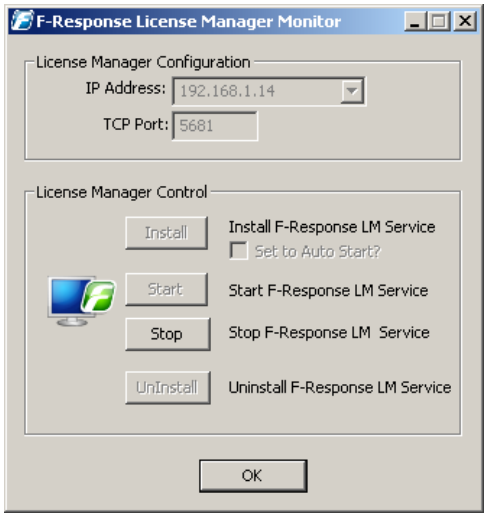
F-Response License Manager Monitor console, Main Window

Install the F-Response License Manager service by pressing the Install button. After the service is installed it will allow you to change the bound IP Address and TCP Port, the service will install in the stopped position.



F-Response License Manager Monitor, Stopped Position

Start the F-Response License Manager service by pressing the Start button. Your F-Response FOB must be inserted prior to starting the License Manager server.



F-Response License Manager running and waiting for licensing requests.

The F-Response License Manager is now running and waiting for licensing requests. The License Manager automatically creates Windows Firewall exceptions for the service application, however if you are using other firewall products you many need to add exceptions as necessary.

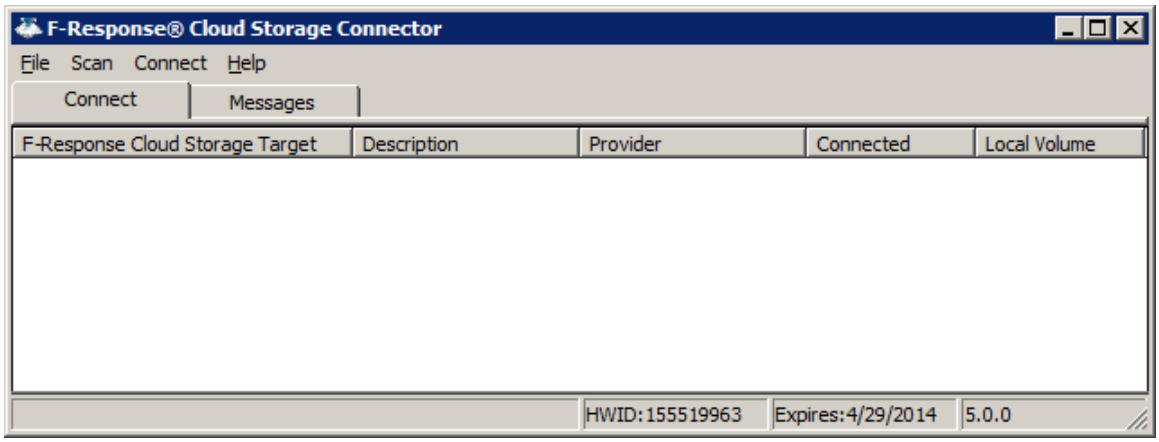
F-Response Cloud Connector

Using the F-Response Cloud Connector (TAC,CE,CE+C, and EE)

F-Response TACTICAL, Consultant, Enterprise and Consultant+Covert edition includes a copy of the F-Response Cloud Connector (FCLDC). The FCLDC allows an examiner to mount remote Cloud based Storage containers as local read-only logical volumes or network shares.

The FCLDC does not require executables or agents be deployed to Cloud Storage providers.

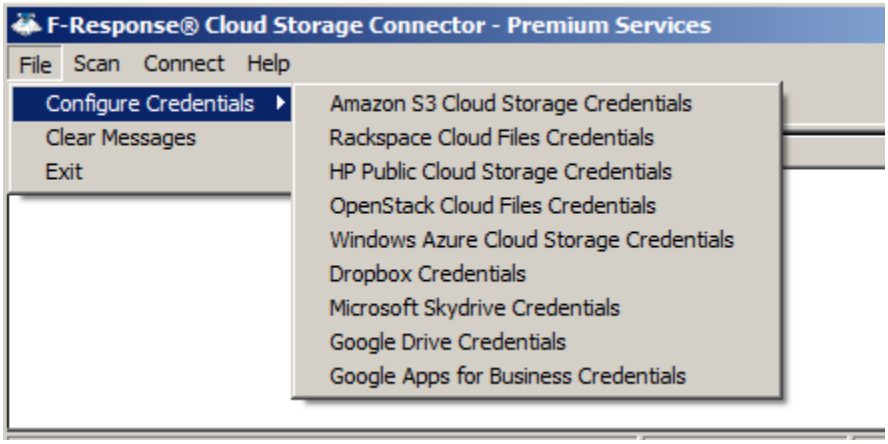
The FCLDC does require a locally attached F-Response licensed dongle (TACTICAL, Consultant, or Consultant+Covert), or a remote Enterprise F-Response dongle connected via the F-Response License Manager at all times.



F-Response Cloud Connector

Configuring Cloud Credentials

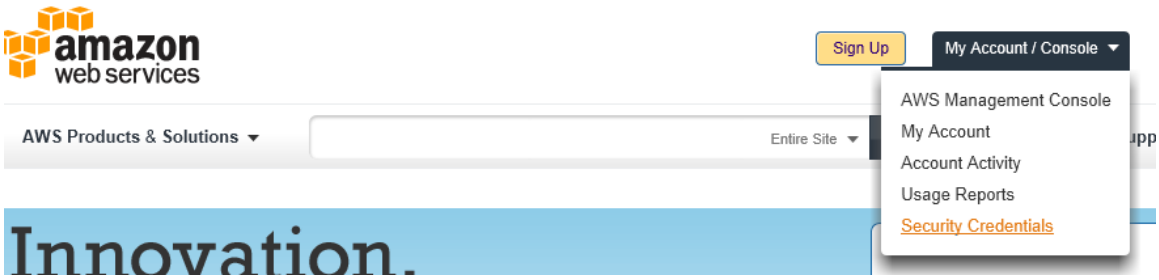
Before you can connect to Cloud Storage services you must first input valid credentials. While the credentials necessary vary by cloud storage provider, all credentials must be input using one of the Configure Credentials dialog boxes.



File->Configure Credentials

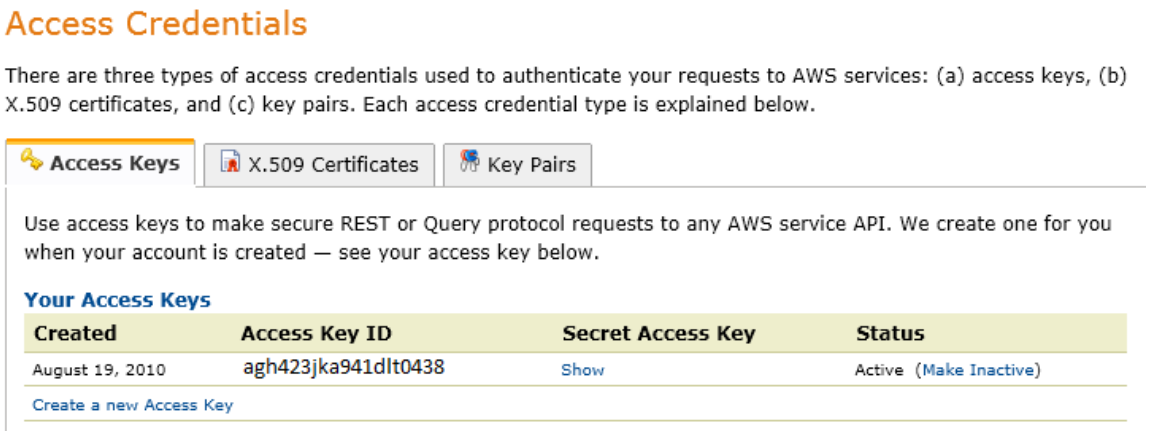
Amazon S3 Cloud Storage Credentials

Amazon S3 Storage Credentials are found on the Amazon AWS Console (see aws.amazon.com). The specific credentials required are available under the "Security Credentials" link under My Account, see below:



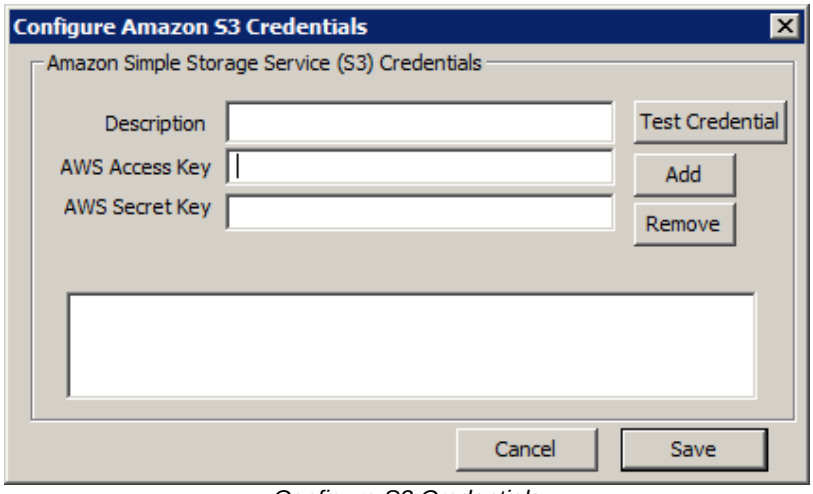
Amazon Web Services Main Page

Locate the "Access Credentials section and record (copy/paste) the Access Key ID, then press "Show" to open a secondary window containing the Secret Access Key.


Access Credentials
There are three types of access credentials used to authenticate your requests to AWS services: (a) access keys, (b) X.509 certificates, and (c) key pairs. Each access credential type is explained below.
Access Keys
X.509 Certificates
Key Pairs
Use access keys to make secure REST or Query protocol requests to any AWS service API. We create one for you when your account is created — see your access key below.
Your Access Keys
Created
Access Key ID
Secret Access Key
Status
August 19, 2010
agh423jka941dlt0438
Show
Active (Make Inactive)
Create a new Access Key

Amazon AWS Access Key and Secret Access Key

The preceding credentials (Access Key and Secret Key) must be entered in the corresponding fields in the Configure S3 Credentials dialog. The Description field is optional and can be used to provide a secondary human readable identifier for the credential set (Ex "Client X Credentials").



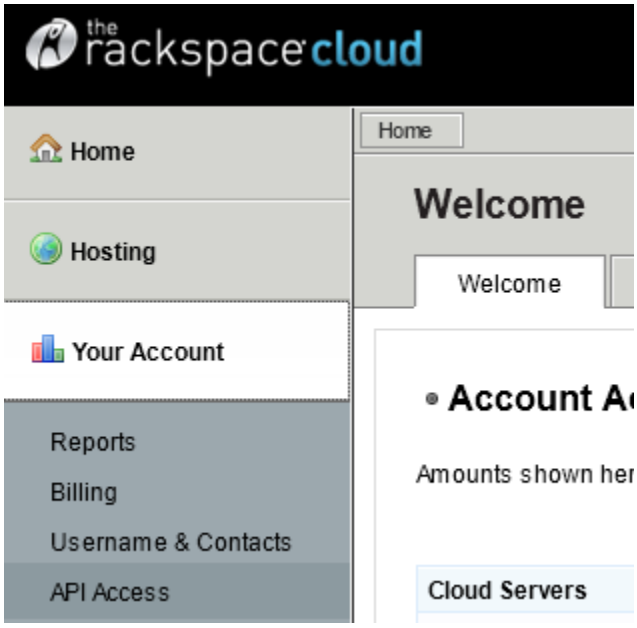
Configure S3 Credentials

Use the "Test Connection" button to test the credentials against Amazon S3. If the credentials are valid you can then use the "Add" button to Add the credentials to your stack of available credentials. Lastly, press "Save" to store the credentials on the examiner machine in an encrypted repository.

It is important to note that all Cloud Storage credentials are saved, unlike the F-Response Enterprise Management Console deployment credentials.

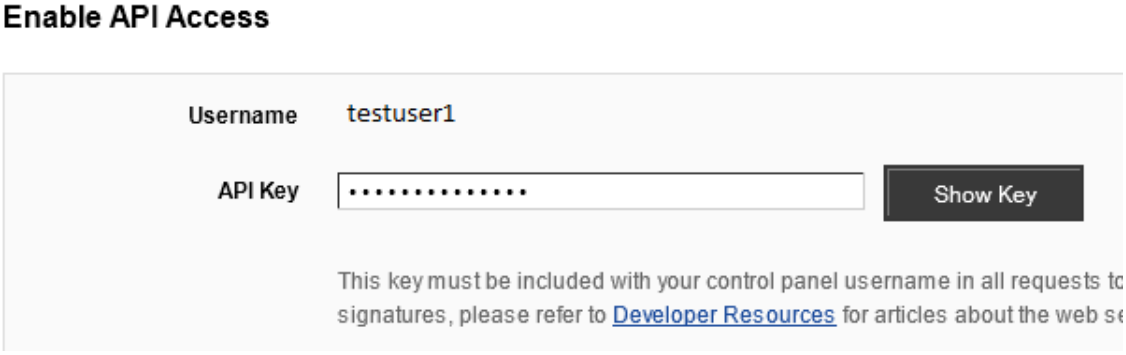
Rackspace Cloud Files Credentials

Rackspace Cloud Files Credentials are found on the Rackspace Management Console (see manage.rackspacecloud.com). The specific credentials required are available under the "Your Account" menu item, under API Access, see below:



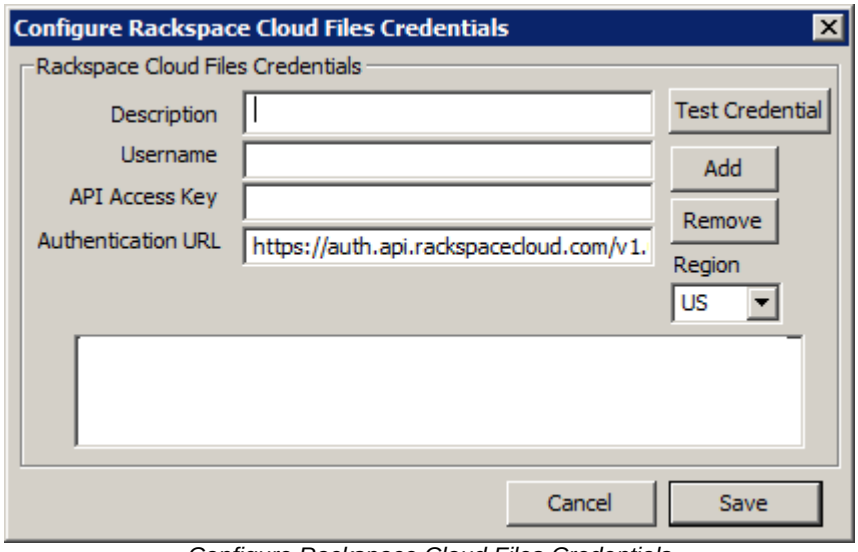
Rackspace Cloud Management Console Main Page

Locate the API Access section and record (copy/paste) the Username, then press "Show Key" to open a secondary window containing the API Key.


Enable API Access
Username
testuser1
API Key
Show Key
This key must be included with your control panel username in all requests to
signatures, please refer to Developer Resources for articles about the web se

Username and API Key

The preceding credentials (Username and API Key) must be entered in the corresponding fields in the Configure Rackspace Cloud Files Credentials dialog. The Description field is optional and can be used to provide a secondary human readable identifier for the credential set (Ex "Client X Credentials"). In addition an Authentication URL must be selected, either US or UK, the drop down is available to the right of the Authentication URL text input. The region is specific to where the account was created, **not** where the examiner is located at present. The default is the US region.



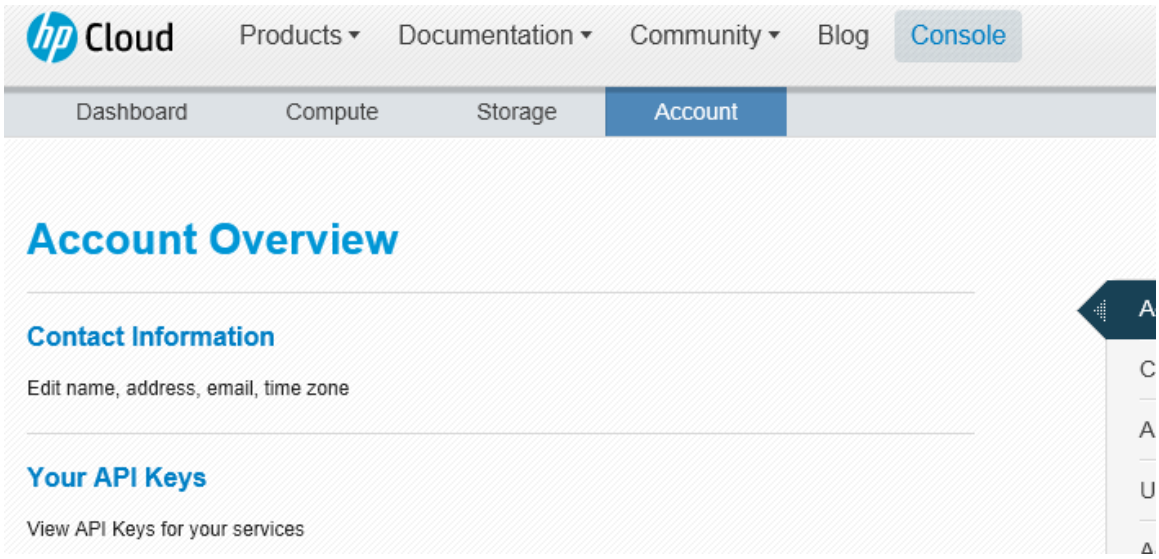
Configure Rackspace Cloud Files Credentials

Use the "Test Connection" button to test the credentials against Rackspace Cloud Files. If the credentials are valid you can then use the "Add" button to Add the credentials to your stack of available credentials, lastly press "Save" to store the credentials on the examiner machine in an encrypted repository.

It is important to note that all Cloud Storage credentials are saved, unlike the F-Response Enterprise Management Console deployment credentials.

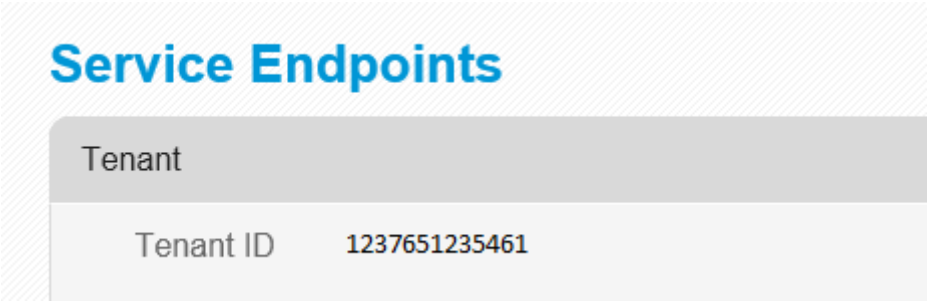
HP Public Cloud Credentials

HP Public Cloud Credentials are found on the HP Public Cloud Console (see console.hpcloud.com). The specific credentials required are available under the "Account" menu item, under "Your API Keys", see below:



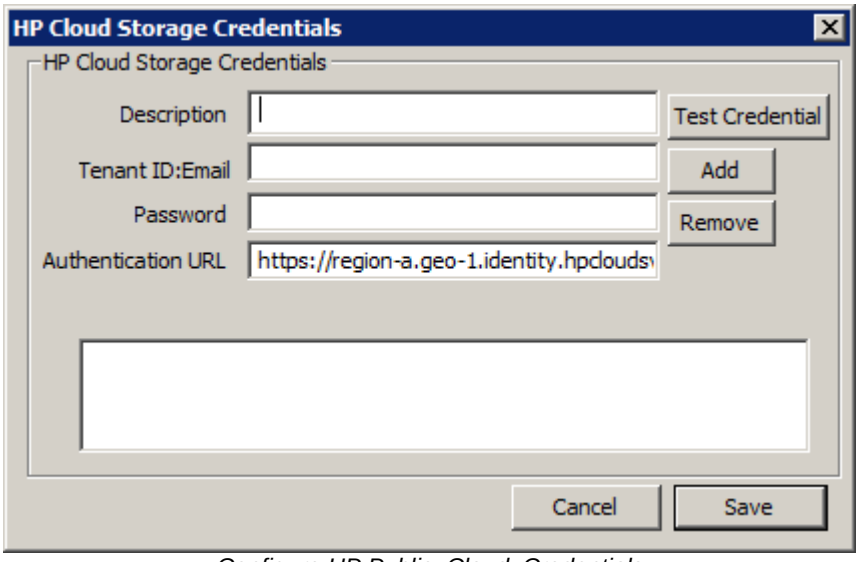
HP Public Cloud Management Console Main Page

Locate the Service Endpoints section and record (copy/paste) the Tenant ID.



Service Endpoints, Tenant ID

The preceding credential (Tenant ID) must be entered along with the login email for the Cloud Console in the corresponding field in the Configure HP Public Cloud Credentials dialog, for example "1237651235461:test@test.com". The Password field requires the password used to login to the HP Public Cloud Web Console. The Description field is optional and can be used to provide a secondary human readable identifier for the credential set (Ex "Client X Credentials").

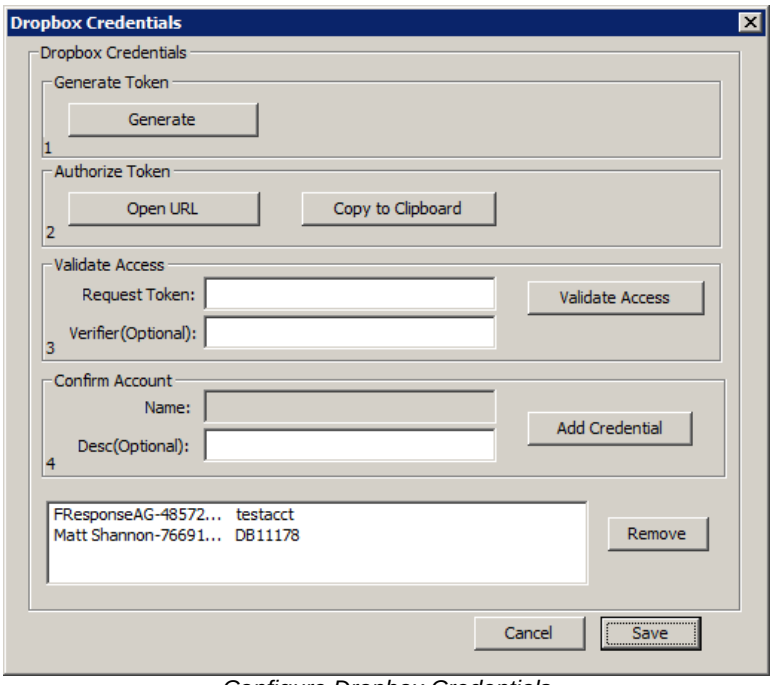


Configure HP Public Cloud Credentials

Use the "Test Connection" button to test the credentials against HP Public Cloud Files. If the credentials are valid you can then use the "Add" button to Add the credentials to your stack of available credentials, lastly press "Save" to store the credentials on the examiner machine in an encrypted repository.

Dropbox Credentials

Dropbox uses the web standard OAUTH for providing application access to accounts. With OAUTH the application user, in this case the F-Response Cloud Connector user does not have knowledge of the Dropbox username or password. Therefore in order to connect the Dropbox using the Cloud Connector the Dropbox user must expressly approve access. The following dialog and details further illustrate this process.



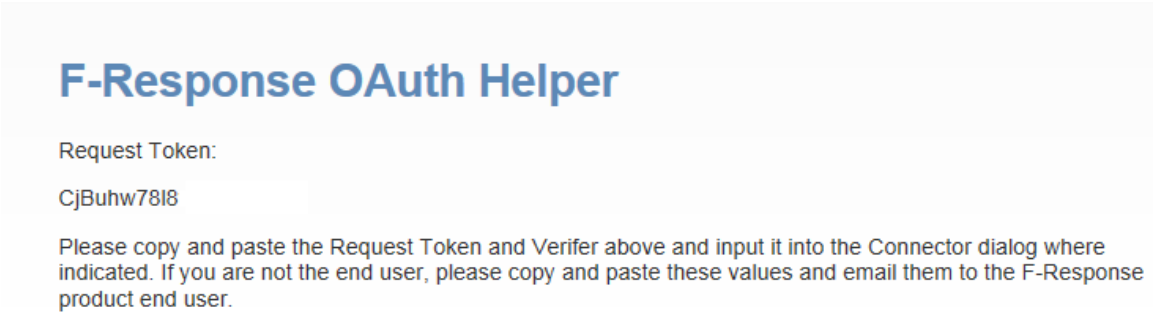
Configure Dropbox Credentials

The first step is to generate a token for requesting credentialed access. An examiner may accomplish this by pressing on the "Generate" button. Upon indication of a successful Token generation the examiner must now get the user to Authorize the newly generated Token. This can be accomplished in one of two ways. Either open the url directly using "Open URL", in this case the examiner will need the username and password as they will be approving access on the account holder's behalf, or use the "Copy to Clipboard" option to generate a URL suitable for sending to the account holder.

The app F-Response Cloud Connector
would like to connect with your Dropbox.
This app will have access to your entire Dropbox.
Please make sure you trust this app before proceeding.
You're currently signed in as . If you meant to connect from another account, you can sign out.
Allow
Deny

User must approve access to the F-Response Cloud Connector

Regardless of the option selected, the account holder must approve access to their Dropbox account, upon approval the web browser will be redirect to a page at F-Response.com with the Request Token and optional Verifier.


F-Response OAuth Helper
Request Token:
CjBuhw78I8
Please copy and paste the Request Token and Verifer above and input it into the Connector dialog where indicated. If you are not the end user, please copy and paste these values and email them to the F-Response product end user.

F-Response.com OAuth Helper Page

The Request Token value (and any optional Verifier) as displayed on that page must be inputted into the Dropbox Credentials dialog in the "Request Token" box. After this is complete, press "Validate Access" to validate the newly acquired Request Token.

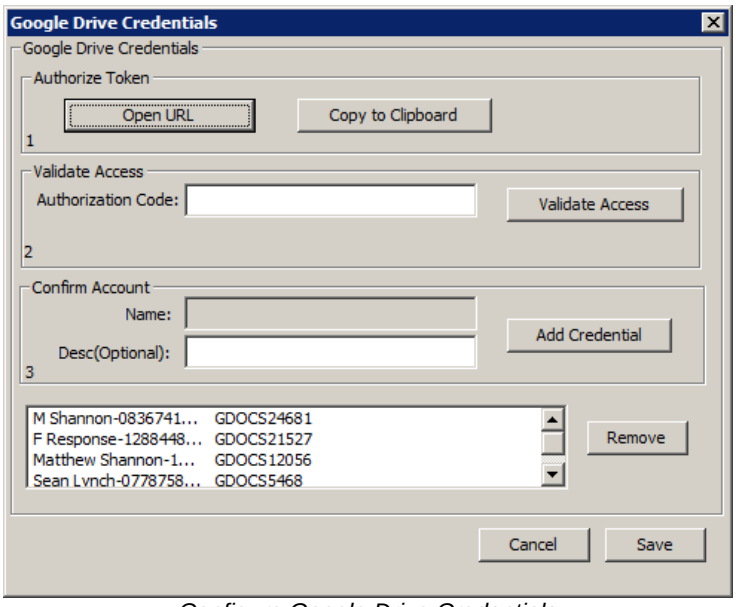
Validate Access will confirm the account holder's account details, and present that information in the "Name" box.

If this is the correct username and account, press "Add" to add the credential to the encrypted credential store and "Save" to save the newly added credential.

It is important to note that all Cloud Storage credentials are saved, unlike the F-Response Enterprise Management Console deployment credentials.

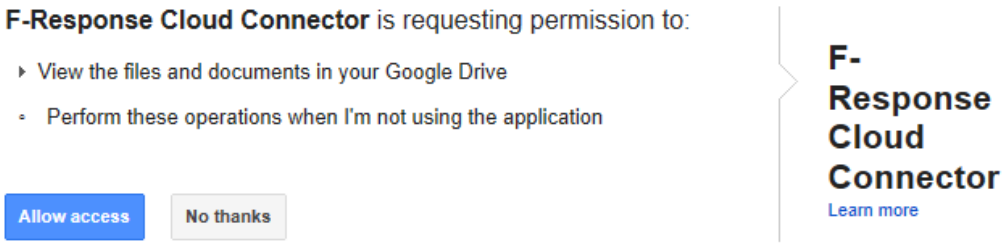
Google Drive Credentials

Google Drive uses the web standard OAUTH2 for providing application access to accounts. With OAUTH2 the application user, in this case the F-Response Cloud Connector user does not have knowledge of the Google Drive username or password. Therefore in order to connect the Google Drive using the Cloud Connector the Google Drive user must expressly approve access. The following dialog and details further illustrate this process.



Configure Google Drive Credentials

The first step is to get the account holder to Authorize the Token. This can be accomplished in one of two ways. Either open the url directly using "Open URL", in this case the examiner will need the username and password as they will be approving access on the account holder's behalf, or use the "Copy to Clipboard" option to generate a URL suitable for sending to the account holder.


F-Response Cloud Connector is requesting permission to:
View the files and documents in your Google Drive
Perform these operations when I'm not using the application
Allow access
No thanks
F-Response Cloud Connector
Learn more

User must approve access to the F-Response Cloud Connector

Regardless of the option selected, the account holder must approve access to their Google Drive account, upon approval the web browser will be redirect to a page at F-Response.com with the Authorization Code.

F-Response OAuth v2 Helper
Authorization Code:
4/ll4UblHsuQbQf_qcnev9dk3Dtfgp.0hsjG
Please copy the Authorization code above and input it into the Connector dialog where indicated. If you are not the end user, please copy the code and email them to the F-Response product end user.

F-Response.com OAuth Helper Page

The Authorization Code as displayed on that page must be inputted into the Google Drive Credentials dialog in the "Authorization Code" box. After this is complete, press "Validate Access".

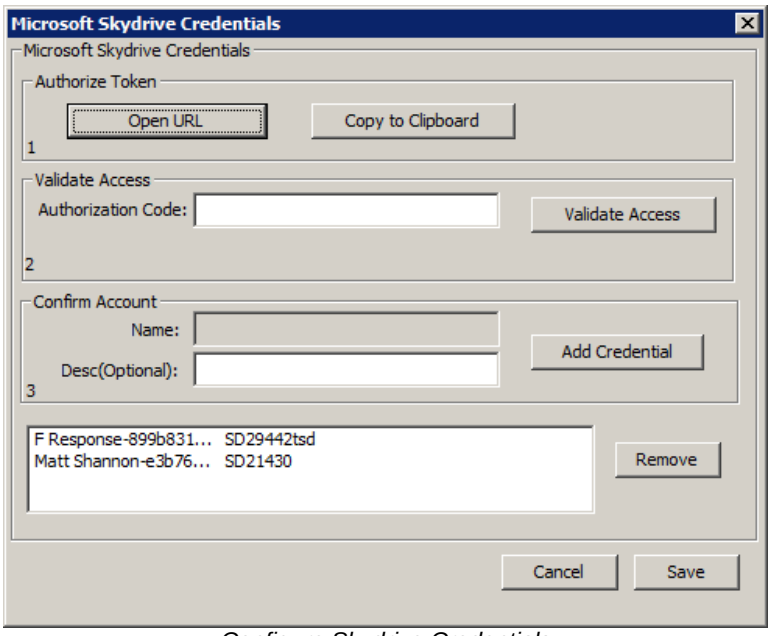
Validate Access will confirm the account holder's account details, and present that information in the "Name" box.

If this is the correct username and account, press "Add" to add the credential to the encrypted credential store and "Save" to save the newly added credential.

It is important to note that all Cloud Storage credentials are saved, unlike the F-Response Enterprise Management Console deployment credentials.

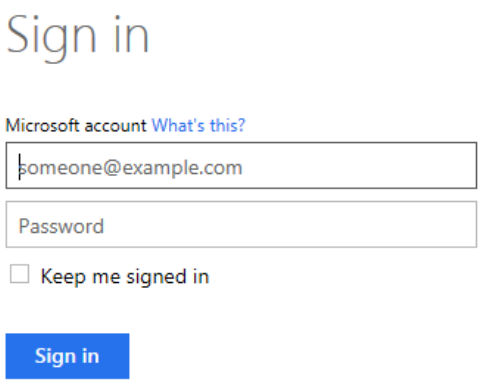
Microsoft Skydrive Credentials

Microsoft Skydrive uses the web standard OAUTH2 for providing application access to accounts. With OAUTH2 the application user, in this case the F-Response Cloud Connector user does not have knowledge of the Skydrive username or password. Therefore in order to connect the Microsoft Skydrive using the Cloud Connector the Skydrive user must expressly approve access. The following dialog and details further illustrate this process.



Configure Skydrive Credentials

The first step is to get the user to Authorize the Token. This can be accomplished in one of two ways. Either open the url directly using "Open URL", in this case the examiner will need the username and password as they will be approving access on the account holder's behalf, or use the "Copy to Clipboard" option to generate a URL suitable for sending to the account holder.



User must approve access to the F-Response Cloud Connector

Regardless of the option selected, the account holder must approve access to their Skydrive account, upon approval the web browser will be redirect to a page at F-Response.com with the Authorization Code.

F-Response OAuth v2 Helper
Authorization Code:
4/ll4UblHsuQbQf_qcnev9dk3Dtfgp.0hsjG
Please copy the Authorization code above and input it into the Connector dialog where indicated. If you are not the end user, please copy the code and email them to the F-Response product end user.

F-Response.com OAuth Helper Page

The Authorization Code as displayed on that page must be inputted into the Skydrive Credentials dialog in the "Authorization Code" box. After this is complete, press "Validate Access".

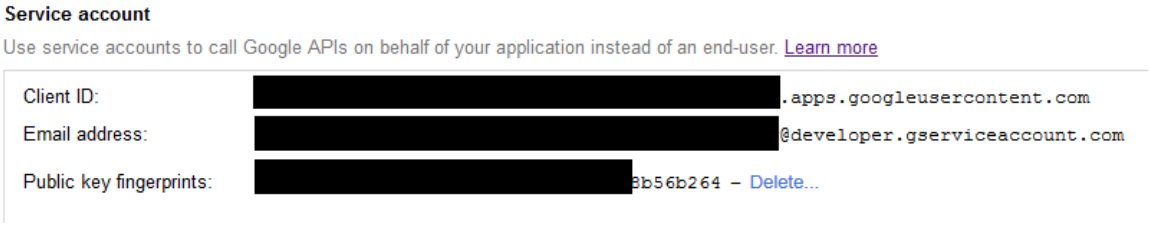
Validate Access will confirm the account holder's account details, and present that information in the "Name" box.

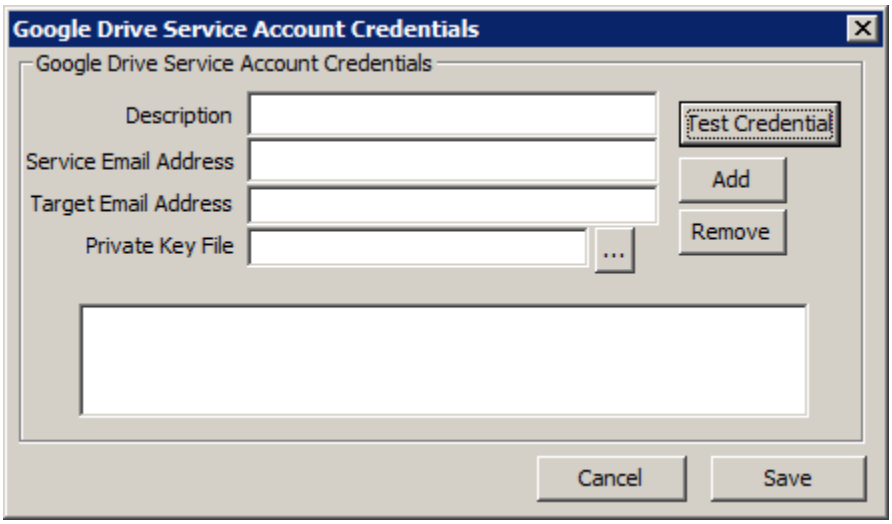
If this is the correct username and account, press "Add" to add the credential to the encrypted credential store and "Save" to save the newly added credential.

It is important to note that all Cloud Storage credentials are saved, unlike the F-Response Enterprise Management Console deployment credentials.

Google Apps for Business Credentials

In addition to consumer class Google Drive access, the F-Response Cloud Connector also includes support for Google Drive Service Account access (Consultant and above only). In this model a Google Apps account administrator has configured Google Drive Read-Only access domain wide for a specific service account. More details on creating that account and delegation are available at the following url (https://developers.google.com/drive/delegation).


Service account
Use service accounts to call Google APIs on behalf of your application instead of an end-user. Learn more
Client ID:
.apps.googleusercontent.com
Email address:
@developer.gserviceaccount.com
Public key fingerprints:
3b56b264 – Delete...



Google Drive Service Account Credentials Dialog

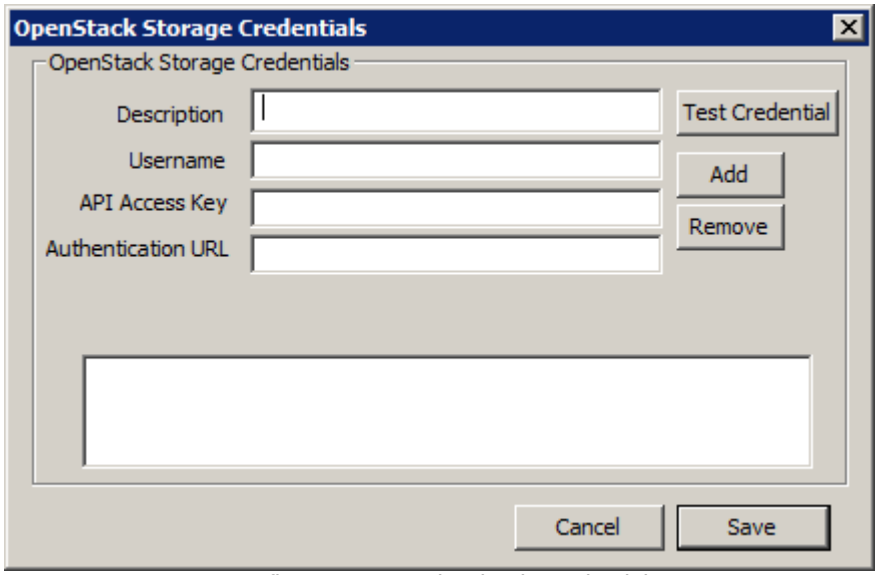
Google Drive Apps/Service Account based cloud storage environments require the following credentials in order to successfully connect and authenticate:

- Service Email Address
  - Service account email address as defined by Google.
- Target Email Address
  - Individual account email address used to identify the target Google Drive repository.
- Private Key File
  - Private key file provided by Google for the Service account.

Openstack Based Cloud Storage

Openstack is an open-source cloud storage platform based on the Rackspace API and model. Openstack based cloud storage environments require the following credentials in order to successfully connect and authenticate:

- Username
  - Provided by the implementer, this may be a simple textual value or may be a generated alphanumeric code.
- API Key
  - Provided by the implementer, this is most likely to be a generated alphanumeric code.
- Authentication URL
  - Provided by the implementer, this URL is necessary to authenticate to the Openstack based cloud storage environment.



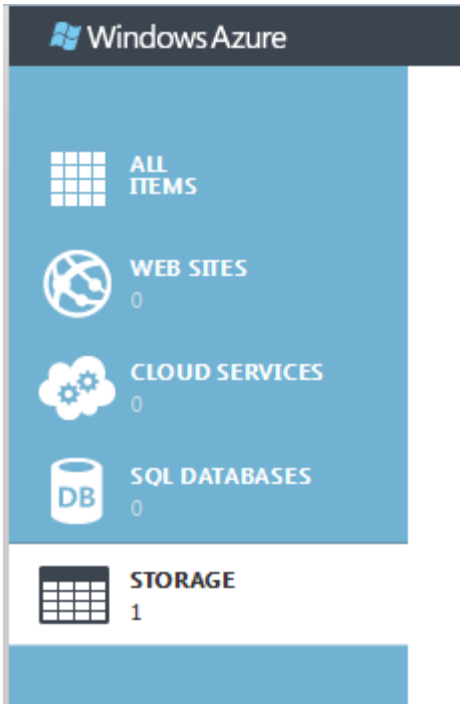
Configure Openstack Cloud Credentials

Use the "Test Connection" button to test the credentials against Openstack based cloud storage environment. If the credentials are valid you can then use the "Add" button to Add the credentials to your stack of available credentials, lastly press "Save" to store the credentials on the examiner machine in an encrypted repository.

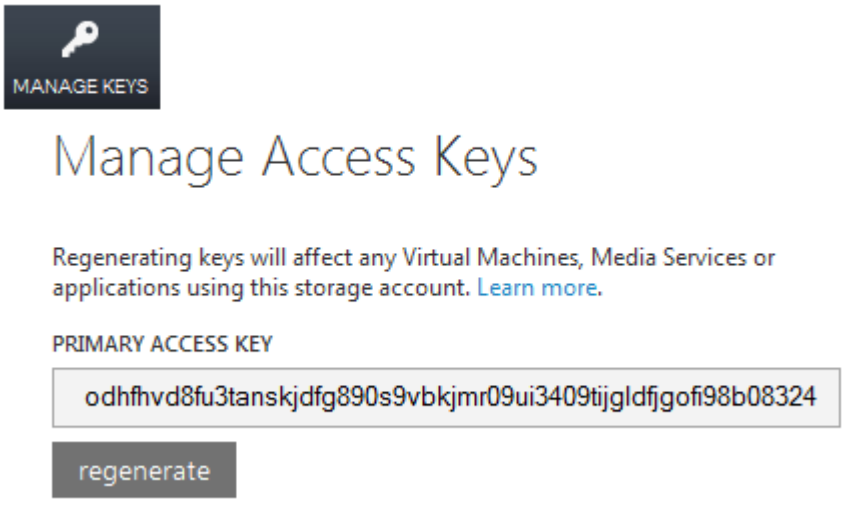
It is important to note that all Cloud Storage credentials are saved, unlike the F-Response Enterprise Management Console deployment credentials.

Windows Azure Blob Storage

Windows Azure Blob Storage Credentials are found on the Windows Azure Console (see www.windowsazure.com, Portal). The specific credentials are available under "Storage" then the "Manage Keys" option at the bottom of the page, see below:

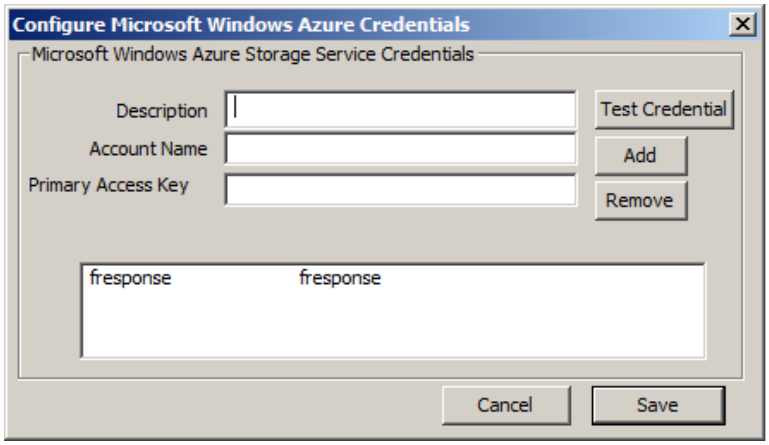


Windows Azure Management Console Main Menu


MANAGE KEYS
Manage Access Keys
Regenerating keys will affect any Virtual Machines, Media Services or applications using this storage account. Learn more.
PRIMARY ACCESS KEY
odhfhvd8fu3tanskjdfg890s9vbkjmr09ui3409tijgldfjgofi98b08324
regenerate

Manage Keys -> Manage Access Keys, Primary Access Key

Microsoft Windows Azure provides both a Primary and Secondary Access key. You can use either of these keys along with the Storage account name to authenticate to the Windows Azure Blob Storage Service. The Password field requires the password used to login to the HP Public Cloud Web Console. The Description field is optional and can be used to provide a secondary human readable identifier for the credential set (Ex "Client X Credentials").



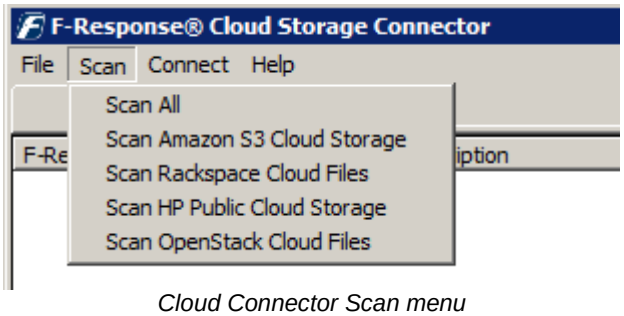
Configure Windows Azure Blob Storage Credentials

Use the "Test Connection" button to test the credentials against Windows Azure Blob Storage. If the credentials are valid you can then use the "Add" button to Add the credentials to your stack of available credentials, lastly press "Save" to store the credentials on the examiner machine in an encrypted repository.

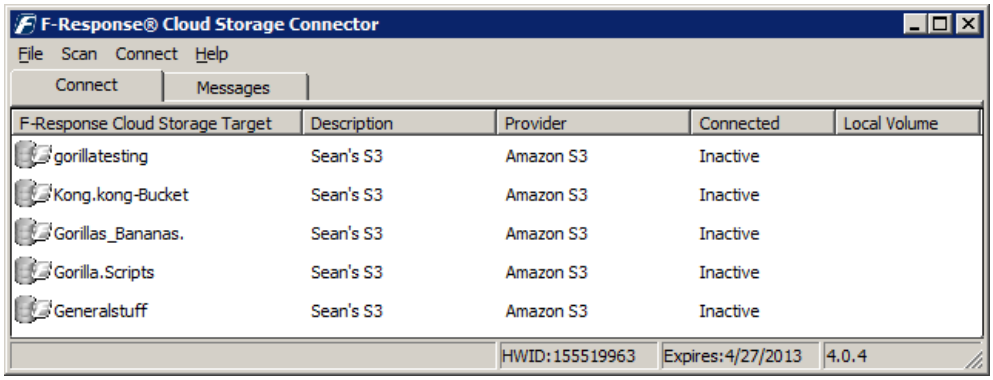
It is important to note that all Cloud Storage credentials are saved, unlike the F-Response Enterprise Management Console deployment credentials.

Scanning for Cloud Storage Targets

Use the Scan menu to enumerate cloud storage containers/buckets by service.



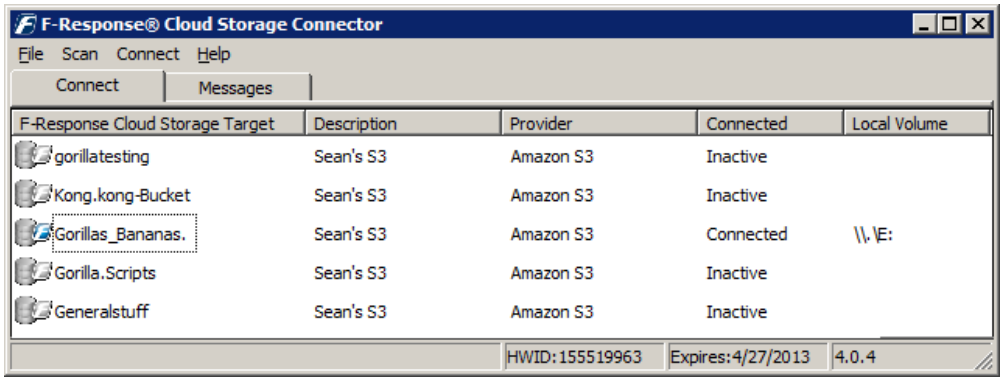
Cloud Connector Scan menu



Cloud Connector scan results

Connecting to Cloud Storage Targets

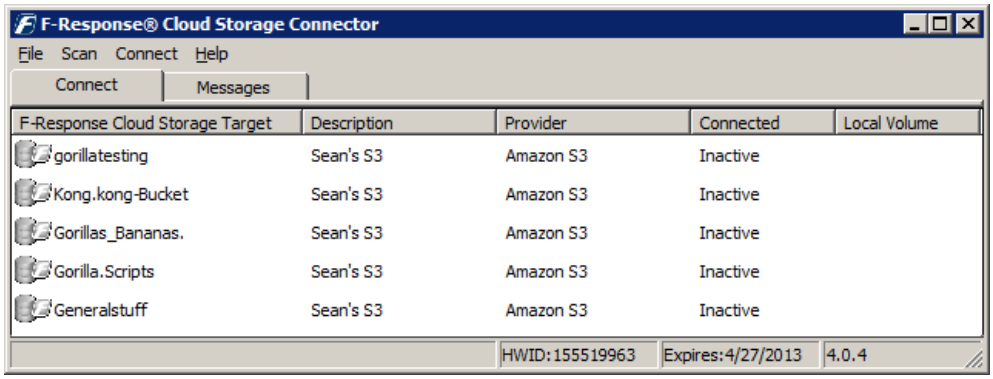
You can connect to a storage target by selecting the target, right clicking to open the context menu, and selecting "Login to F-Response Cloud Storage Volume". The newly attached volume will be assigned a drive letter and is now accessible via Windows Explorer.



Logged in Cloud Storage target assigned the E:\ drive letter

Disconnecting from Cloud Storage Targets

You can disconnect from a storage target by selecting the target, right clicking to open the context menu, and selecting "Logout of F-Response Cloud Storage Volume". The volume will be disconnected and the assigned drive letter will now be removed.



Logged in Cloud Storage target assigned the E:\ drive letter

F-Response Database Object Connector

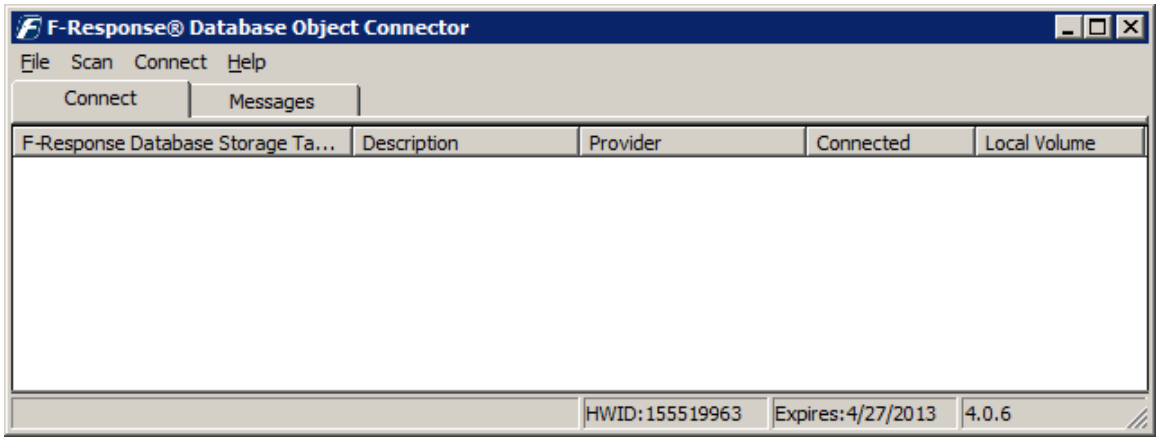
Using the F-Response Database Object Connector (TAC,CE,CE+C, and EE)

F-Response TACTICAL, Consultant, Enterprise and Consultant+Covert edition includes a copy of the F-Response Database Object Connector (FDBC). The FDBC allows an examiner to mount remote Microsoft SQL Server Database Objects (Embedded Files, BLOBS, etc) as local read-only logical volumes or network shares.

The F-Response Database Object Connector supports Microsoft Sharepoint only at present.

The FDBC does not require executables or agents be deployed to the remote Microsoft SQL Server(s).

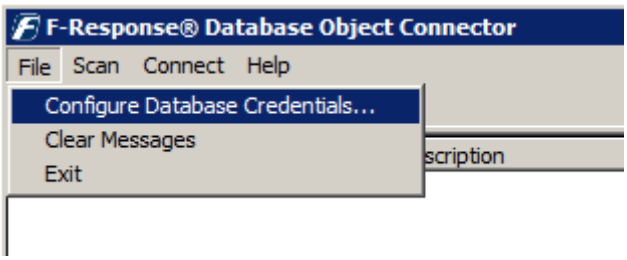
The FDBC does require a locally attached F-Response licensed dongle (TACTICAL, Consultant, or Consultant+Covert), or a remote Enterprise F-Response dongle connected via the F-Response License Manager at all times.



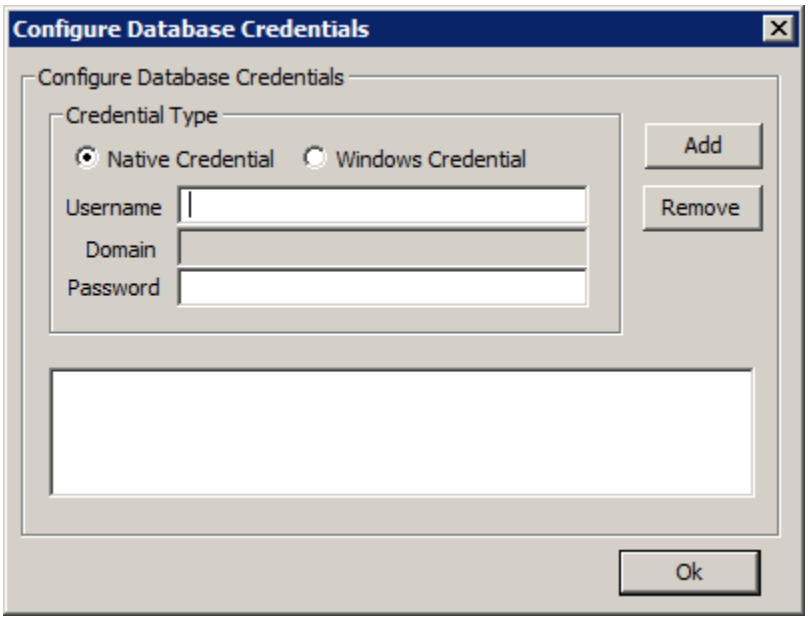
F-Response Database Object Connector

Configuring Database Server Credentials

Before you can connect to Database Server you must first input valid credentials. The current version of the FDBC supports Microsoft SQL Server only, however future versions will allow you to connect to other SQL based servers (including Oracle, etc). The Database Credentials dialog will allow you to enter one or more Database credentials, either Database Native Credentials (SQL Native) or Windows Domain Credentials. Database Credentials are ***not saved*** between executions of the FDBC.



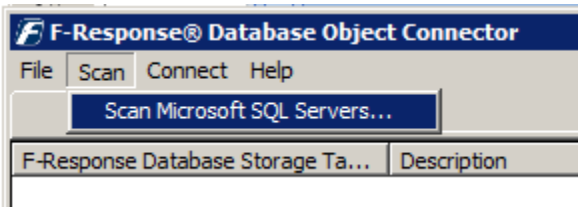
File->Configure Database Credentials…



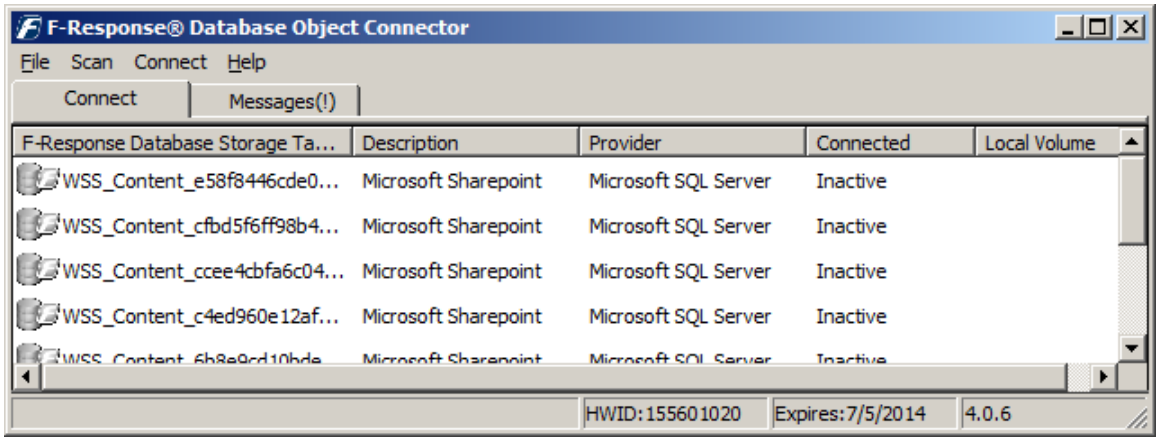
Database Credential dialog, Credentials can be either native credentials (Microsoft SQL Server Native Accounts) or Windows Credentials

Scanning for Database Object Targets

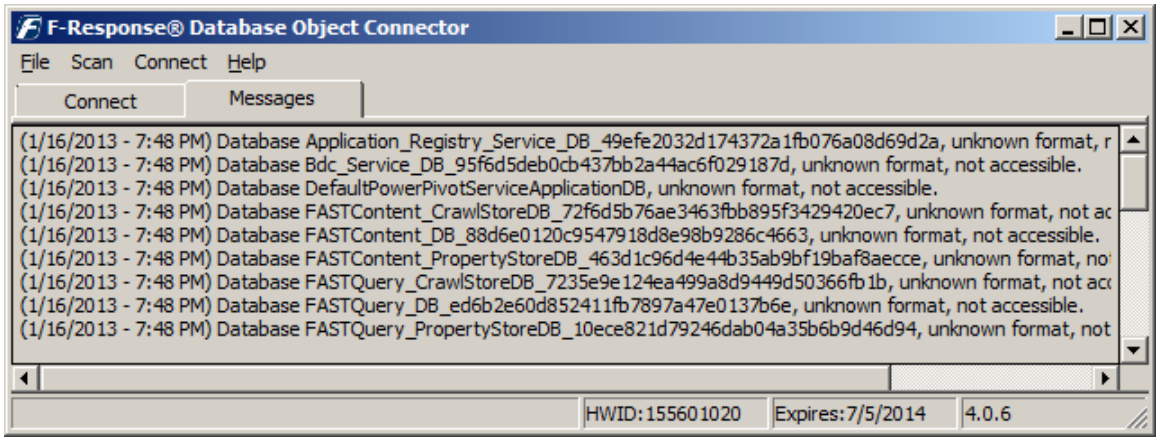
Use the Scan menu to enumerate Microsoft SQL Servers and Databases. The scanning process will use the local "plugins.xml" file to test database format and table structure. Periodically new "plugins.xml" files will be placed on the F-Response Website to add support for new Database formats and models.



Database Object Connector Scan menu



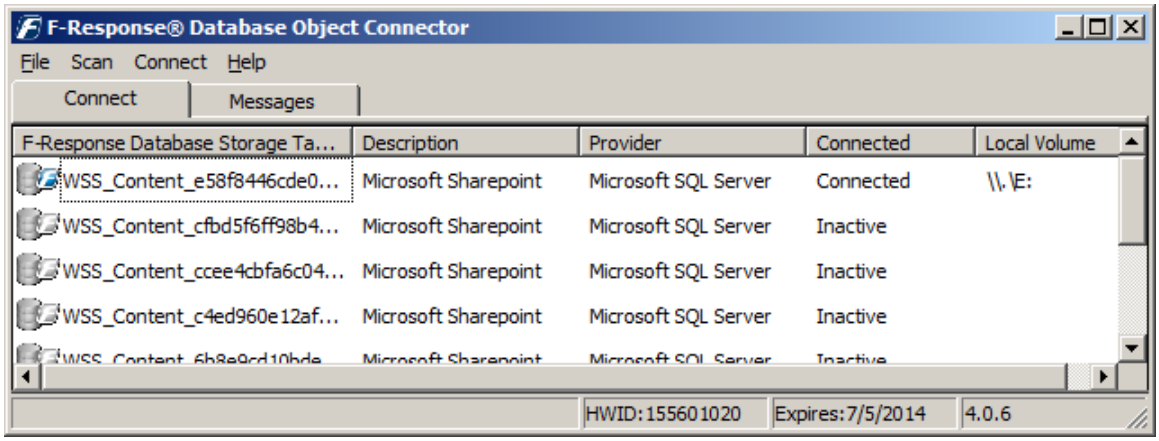
Database Object Connector scan results


F-Response® Database Object Connector
File
Scan
Connect
Help
Connect
Messages
(1/16/2013 - 7:48 PM) Database Application_Registry_Service_DB_49efe2032d174372a1fb076a08d69d2a, unknown format, r
(1/16/2013 - 7:48 PM) Database Bdc_Service_DB_95f6d5deb0cb437bb2a44ac6f029187d, unknown format, not accessible.
(1/16/2013 - 7:48 PM) Database DefaultPowerPivotServiceApplicationDB, unknown format, not accessible.
(1/16/2013 - 7:48 PM) Database FASTContent_CrawlStoreDB_72f6d5b76ae3463fbb895f3429420ec7, unknown format, not ac
(1/16/2013 - 7:48 PM) Database FASTContent_DB_88d6e0120c9547918d8e98b9286c4663, unknown format, not accessible.
(1/16/2013 - 7:48 PM) Database FASTContent_PropertyStoreDB_463d1c96d4e44b35ab9bf19baf8aecce, unknown format, no
(1/16/2013 - 7:48 PM) Database FASTQuery_CrawlStoreDB_7235e9e124ea499a8d9449d50366fb1b, unknown format, not ac
(1/16/2013 - 7:48 PM) Database FASTQuery_DB_ed6b2e60d852411fb7897a47e0137b6e, unknown format, not accessible.
(1/16/2013 - 7:48 PM) Database FASTQuery_PropertyStoreDB_10ece821d79246dab04a35b6b9d46d94, unknown format, not
HWID:155601020
Expires:7/5/2014
4.0.6

Databases not recognized are listed on the Messages Panel

Connecting to Database Object Targets

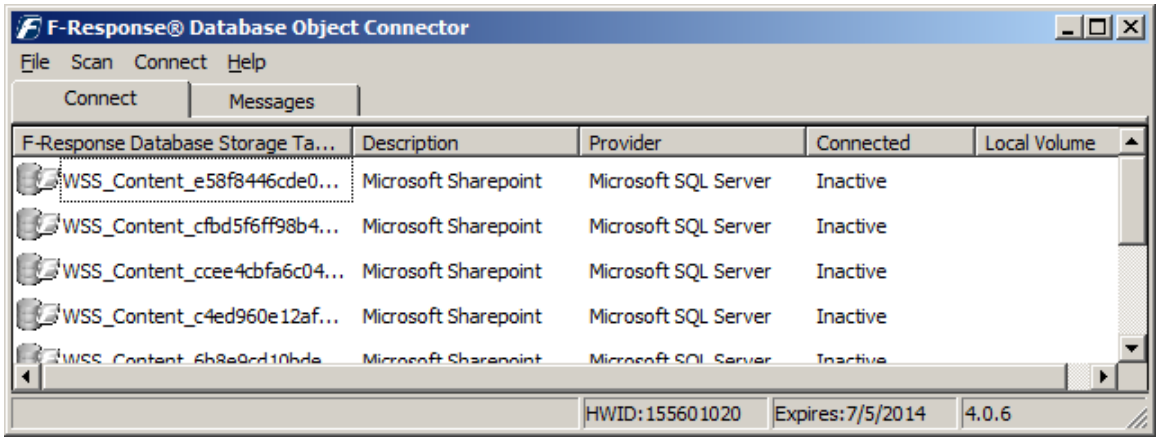
You can connect to a storage target by selecting the target, right clicking to open the context menu, and selecting "Login to F-Response Database Volume". The newly attached volume will be assigned a drive letter and is now accessible via Windows Explorer.



Logged in Database Storage target assigned the E:\ drive letter

Disconnecting from Database Object Targets

You can disconnect from a storage target by selecting the target, right clicking to open the context menu, and selecting "Logout of F-Response Database Volume". The volume will be disconnected and the assigned drive letter will now be removed.



Logged out of the Database Volume

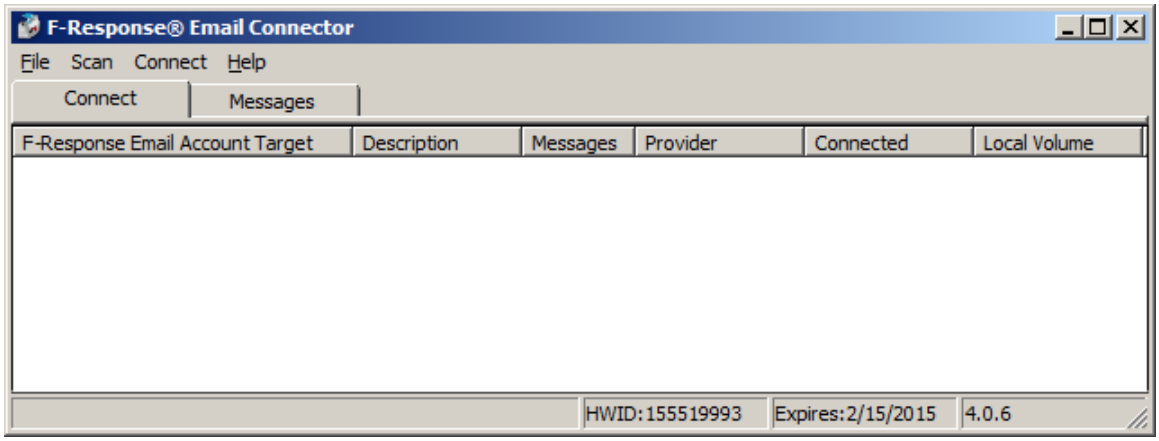
F-Response Email Connector

Using the F-Response Email Connector (TAC,CE,CE+C, and EE)

F-Response TACTICAL, Consultant, Enterprise and Consultant+Covert edition includes a copy of the F-Response Email Connector (FEMLC). The FEMLC allows an examiner to mount remote IMAP based mail storage as local read-only logical volumes or network shares. It also allows an examiner to mount remote Office365 (Exchange Web Services) account data, including emails, calendars, and contacts. The end result of the mapping will be a local read-only volume containing the IMAP folders and individual email messages as ".eml" files, calendar entries, and contacts.

The FEMLC does not require executables or agents be deployed to the remote servers.

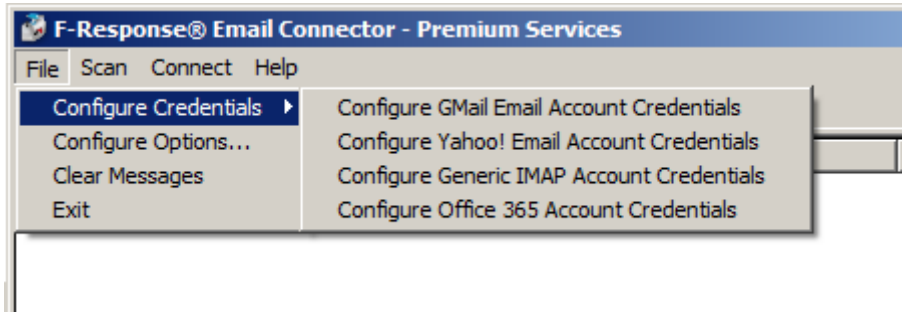
The FEMLC does require a locally attached F-Response licensed dongle (TACTICAL, Consultant, or Consultant+Covert), or a remote Enterprise F-Response dongle connected via the F-Response License Manager at all times.



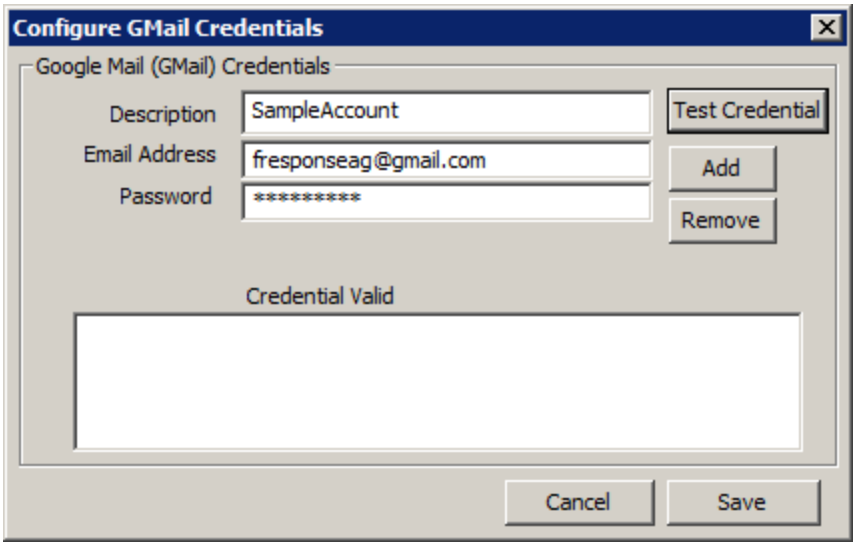
F-Response Email Connector

Configuring Email Credentials

Before you can connect to Email service you must first input valid credentials. The FEMLC supports Gmail, Yahoo! Mail, most generic IMAP servers, and Office 365 native Exchange Web Services. Credentials can be tested before they are added using the "Test Credential" button. Once the credential has been validated press the "Add" button to add them to the list of credentials to be used, then press "Save" to exit the dialog. Email credentials are ***not saved*** between executions of the FEMLC.



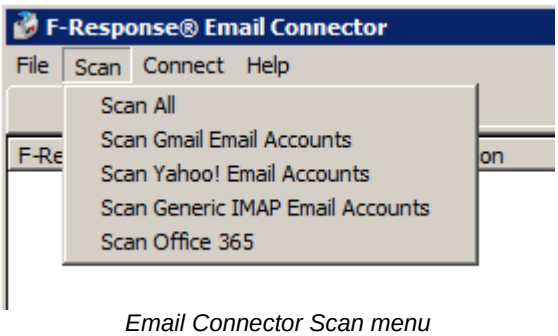
File->Configure Credentials…



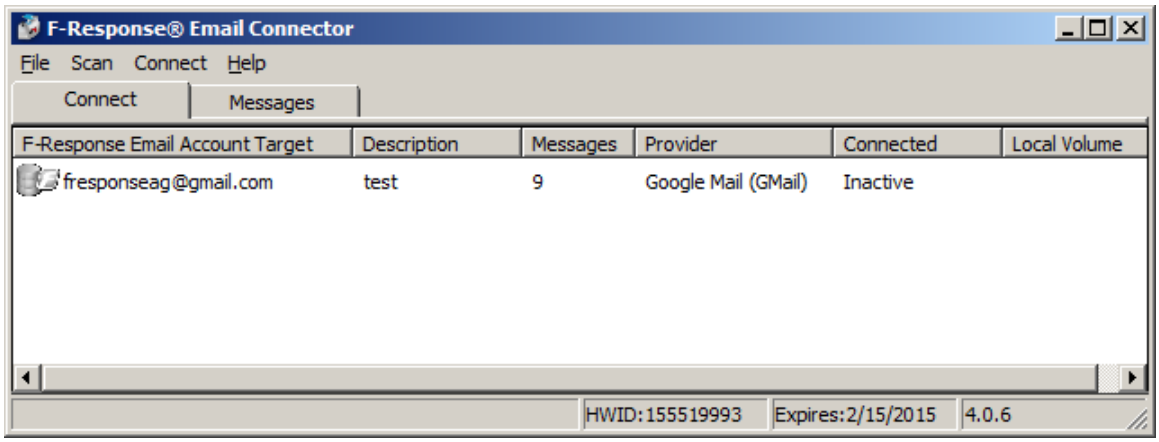
Configure Gmail Credentials Dialog

Scanning for Email Account Targets

Use the Scan menu to enumerate Email servers and accounts.



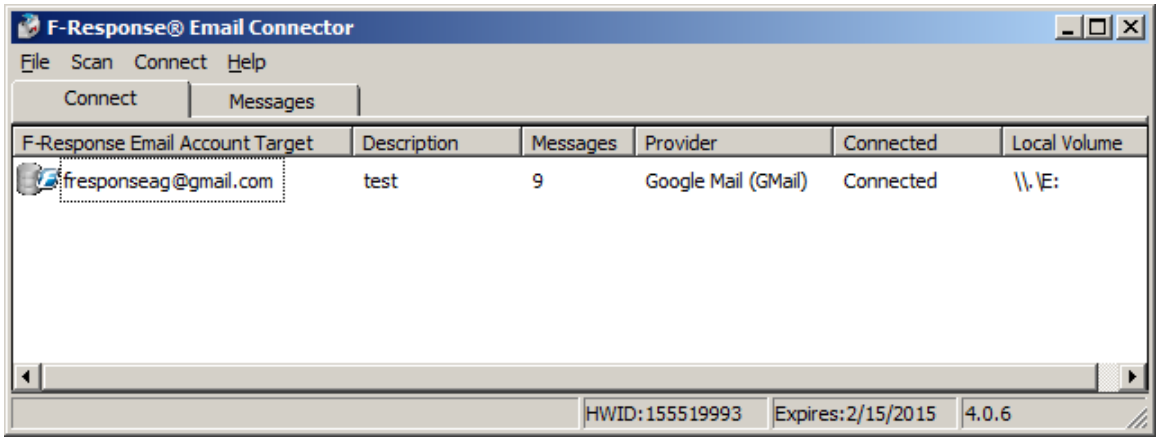
Email Connector Scan menu



Email Connector scan results

Connecting to Email Account Targets

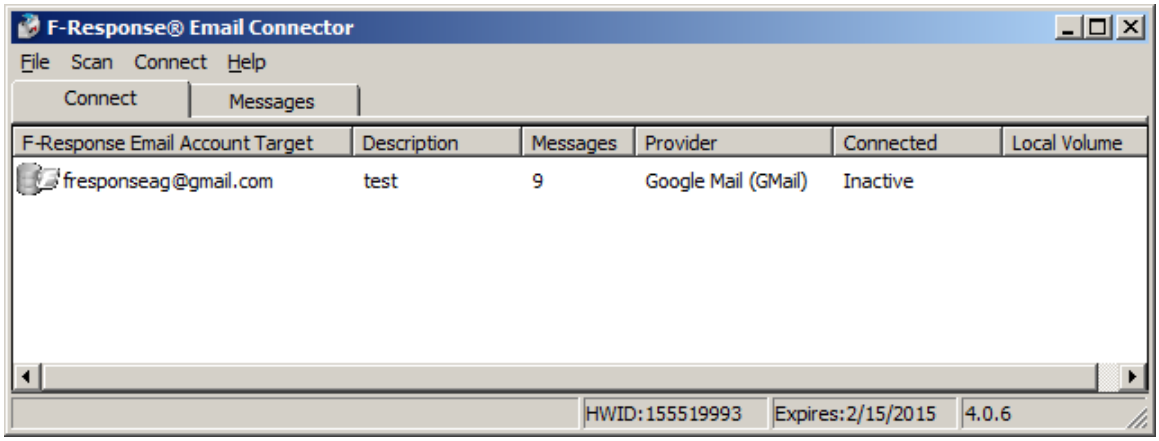
You can connect to a storage target by selecting the target, right clicking to open the context menu, and selecting "Login to F-Response Email Volume". The FEMLC will begin processing the remote email and building a local cache. This process may be stopped at any time using the "Cancel Login to F-Response Email Volume" option. Cancelled processes are restarted on the next "Login…" operation. The processing phase can take a considerable amount of time depending on the total number of messages, size of the messages, available bandwidth, and any throttling of performance done by the email provider. Once complete, the newly attached volume will be assigned a drive letter and is now accessible via Windows Explorer.



Logged in Email Account target assigned the E:\ drive letter

Disconnecting from Email Account Targets

You can disconnect from a storage target by selecting the target, right clicking to open the context menu, and selecting "Logout of F-Response Email Volume". The volume will be disconnected and the assigned drive letter will now be removed.

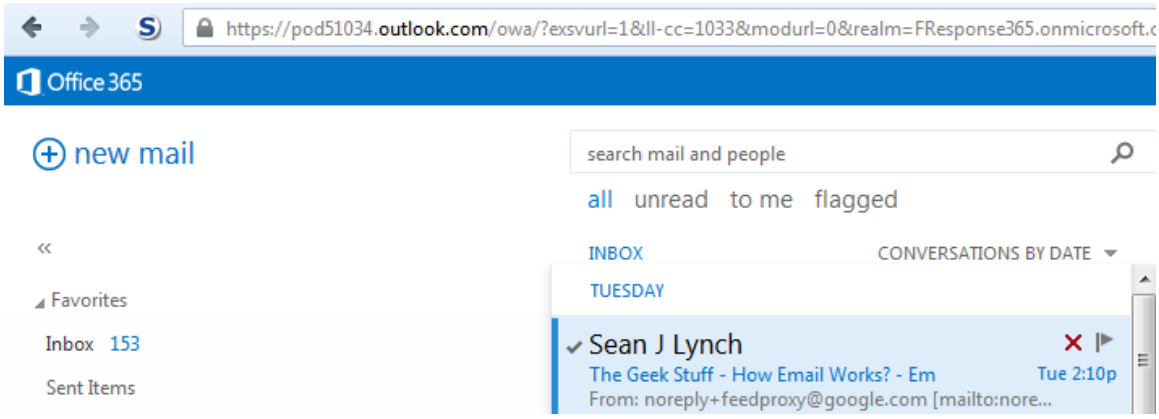


Logged out of the Email Volume

Microsoft Office 365 – Native Exchange Web Services

In addition to IMAP support, the F-Response Email Connector also includes support for Office 365 using native exchange web services. This support is only available for F-Response Consultant edition and above customers.

In order to access Office 365 data you will need the email address, password, and the specific exchange server hosting the Office 365 account. This can be determined using the Office 365 web interface. Refer to the URL bar when accessing Office365 email to determine the appropriate server for the requested account.

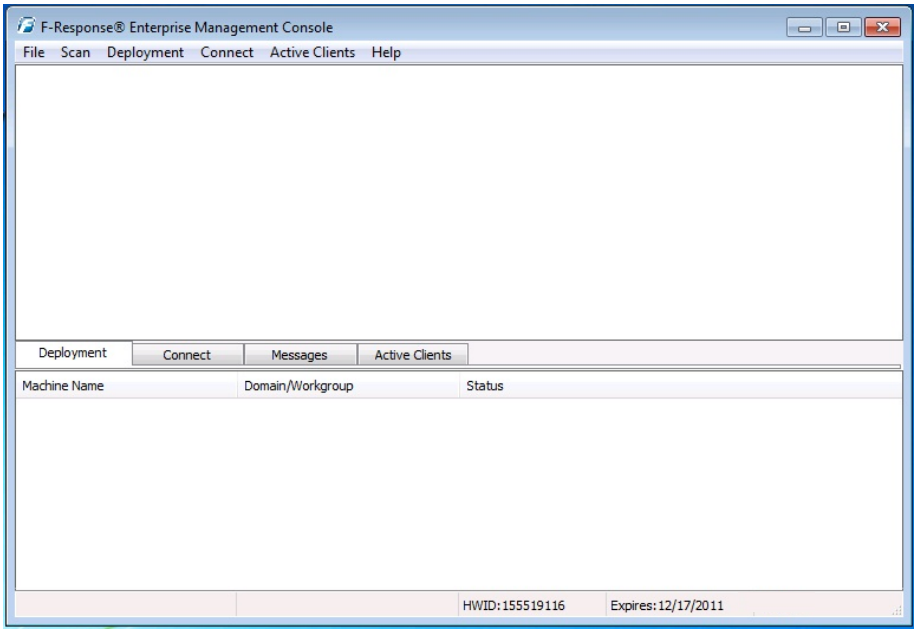


The above example indicates the server hosting that Office365 account is "pod51034.outlook.com".

F-Response Enterprise

Enterprise Edition – Overview of the F-Response Enterprise Management Console (FEMC)

At the core of F-Response Enterprise Edition is the F-Response Enterprise Management Console (FEMC). Below is a guideline of the features and functions of the FEMC.



F-Response Enterprise Management Console

Menu Options

- File
  - Configure:
    - Configure F-Response EMC for deploying and managing Remote F-Response Target code.
  - Clear Messages:
    - Clears any information or error messages currently in the Messages Panel.
  - Exit:
    - Close and exit the F-Response EMC.
- Scan
  - Scan by Domain…
    - Opens a dialog for Windows Domain/Workgroup scanning to detect F-Response Enterprise installations and/or potential targets.
  - Scan by IP Address…
    - Opens a dialog for IP Address range scanning to detect F-Response Enterprise installations and/or potential targets.
  - Direct Connect…

        - Opens a dialog for direct connect options for directly connecting to a remote computer via IP address or Network Name to detect F-Response Enterprise installations and/or potential targets.
    - Custom Scan…
        - Opens a dialog for inputting a comma delineated listing of either computer names or IP addresses (or both) to scan to detect F-Response Enterprise installations and/or potential targets.
- Deployment
    - Install/Start F-Response
        - Installs and then automatically starts F-Response Enterprise on the selected computer(s).
    - Stop/Remove F-Response
        - Stops then removes F-Response Enterprise from the selected computer(s).
    - Install F-Response
        - Installs F-Response Enterprise on the selected computer(s).
    - Uninstall F-Response
        - Uninstalls F-Response Enterprise from the selected computer(s).
    - Start F-Response
        - Starts F-Response Enterprise on the selected computer(s).
    - Stop F-Response
        - Stops F-Response Enterprise on the selected computer(s).
    - Issue Discovery Request
        - Issues an iSCSI Discovery request against the selected computer(s) or Active Client(s).
    - Open F-Response Flexdisk™
        - Opens the default web browser to connect to the selected computer on the Flexdisk™ configured port (HTTPS).
- Connect
    - Discovery F-Response Disks…
        - Opens a dialog providing iSCSI Discovery request capability by IP Address.
    - Login to F-Response Disk
        - Initiates an iSCSI login on the selected F-Response Enterprise Target.
    - Logout of F-Response Disk
        - Initiates an iSCSI logout on the selected F-Response Enterprise Target.
    - Remove F-Response Disk
        - Deletes F-Response Target entries for the selected machine from the Connect Tab.
- Active Clients
    - Poll Continuously
        - Enables or Disables the continuous polling of the F-Response License Manager. If this menu option is unchecked the Active Clients panel will not accurately reflect Active Clients unless the Refresh menu option is used.
    - Refresh
        - Refreshes the Active Clients panel, only available if Poll Continuously is unchecked.
- Help
    - About

- Presents a splash screen indicating the version information of the F-Response Enterprise Management Console (FEMC).

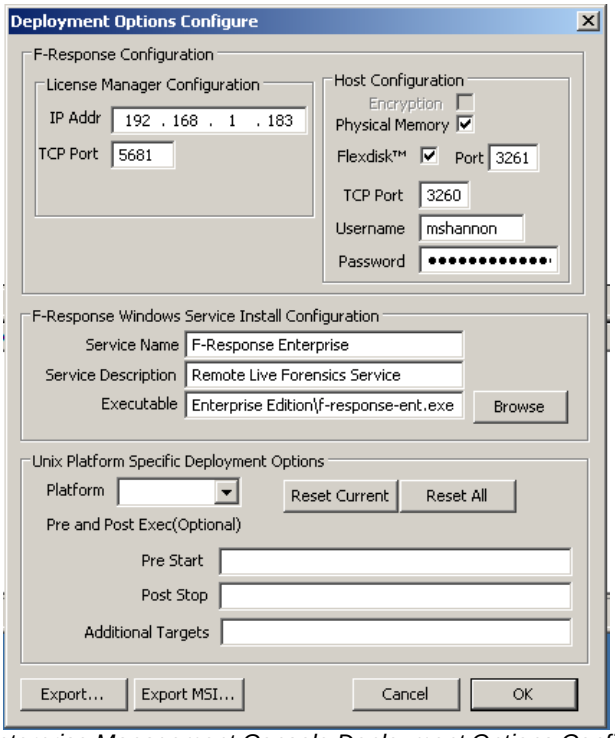
Tab Controls

- Deployment
  - Displays a listing of the computer(s) capable of administration, as well as their Domain/Workgroup and current status.
- Connect
  - Displays a listing of the F-Response Target(s) after a successful Discovery Request.
- Messages
  - Displays informational Messages during operation, if errors occur they will be noted here.
- Active Clients
  - Queries the F-Response License Manager Service to obtain active clients for the F-Response LM dongle. This list includes IP Address, Network Name, and Platform.

Enterprise Edition – Configuring the FEMC Deployment Options

Prior to beginning any operations with F-Response Enterprise Management Console you must complete the Deployment Options Configure dialog. All information inputted will be saved and restored on future usages. In many cases you may only need to enter this information once.

Please refer to the guidelines below for configuring the FEMC Deployment Options.



F-Response Enterprise Management Console Deployment Options Configuration Panel

- F-Response Configuration
  - Validation Configuration
    - IP Addr:
      - Configures the IP Address of the F-Response LM Service.
    - TCP Port:
      - Configures the TCP Port of the F-Response LM Service.
  - Host Configuration
    - Encryption[5]
      - Check to enable AES 256bit Encryption for the F-Response Disk connection.
    - Physical Memory
      - Check to enable Physical Memory access on the remote F-Response Target (Supports Windows clients only).
    - Flexdisk™ Port / Checkbox

[5] Only supported on analyst machines running Microsoft Windows Vista or above, if not supported option will be grayed out.

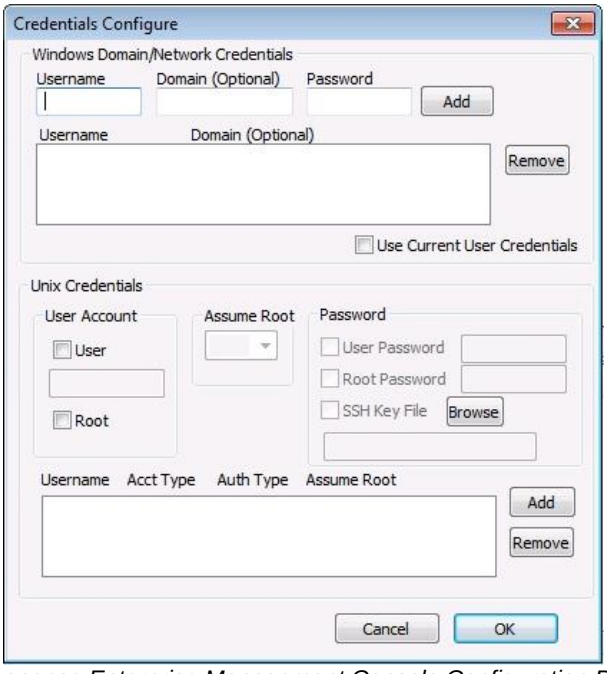
        - The TCP Port the remote F-Response Enterprise executable should listen on for Flexdisk™ (HTTPS) requests.
    - TCP Port
        - The TCP Port the remote F-Response Enterprise executable should listen on for login and discovery requests.
    - Username
        - The Username the remote F-Response Enterprise executable should use for login and discovery requests.
    - Password
        - The Password the remote F-Response Enterprise executable should use for login and discovery requests.
- F-Response Windows Service Install Configuration:
    - Service Name
        - This is the name the F-Response Enterprise service will be installed as on the remote computer(s). This name is completely user selectable.
    - Service Description
        - Description value that will be assigned to the F-Response Enterprise service when installed on the remote computer(s). This description is completely optional.
    - Executable
        - Use the browse button to locate the F-Response Enterprise executable to install (Typically located in C:\Program Files\F-Response\F-Response Enterprise Edition\f-response-ent.exe).
- Unix Platform Specific Options (ADVANCED)
    - A platform based set of options that will be executed on the remote computer, any changes made to the options are saved. Optionally they can be reset using the "Reset Current" or "Reset All" buttons. For additional information see the F-Response Unix Platform options Appendix.
        - Pre Start
            - This is a shell command that will be run prior to starting F-Response on the remote target.
        - Post Stop
            - This is a shell command that will be run directly after stopping F-Response on the remote target.
        - Additional Targets
            - This option will allow you to specify additional targets that may not be detected automatically.
- Export
    - This button will open a file save dialog box to export the configuration information. This is useful when you need to deploy F-Response Enterprise via alternate means. For more information on this process see Enterprise Edition – Using F-Response Enterprise Edition for Windows (Deployment without the FEMC).
- Export MSI
    - This button will open a file save dialog box to export a MSI installer pre-configured with the appropriate configuration and settings. This MSI installer can be used with any deployment application that support MSI based installations, including Windows Active Directory Group Policy.

Enterprise Edition – Configuring the FEMC Credentials

After completing the Deployment Options Config dialog, the next step is to configure the F-Response target(s) login credentials via the Credentials Configure dialog . All information inputted will not be saved or pre-populated for future usages. For obvious reasons credentials are not stored when the application is exited.

The Credentials Configure window is divided into two areas to provide credential information for F-Response targets: Windows Domain/Network Credentials and Unix Credentials.

Please refer to the guidelines below for configuring the FEMC target Credentials.



F-Response Enterprise Management Console Configuration Panel

- Windows Domain/Network Credentials
  - Use the Add/Remove buttons to add and/or remove both Domain and Local machine credentials. These credentials will be used to manage the remote F-Response Target computer, including Install, Start, Stop, and Uninstall operations.
  - Use Current User Credentials
    - This option removes the inputted credentials in favor of using the locally logged in user's credentials.

- Unix Credentials:
    - User Account
      - Provides options for entering user account name and/or type.
    - Assume Root

- Allows for selecting a manner with which to assume "root" privileges, further details on Unix Credentials is available in the Appendix E – Understanding Unix Credentials.

- Password
  - Provides the options for entering User or Root passwords, along with the option for using an SSH Key file (Putty or OpenSSH).

Enterprise Edition – Scanning

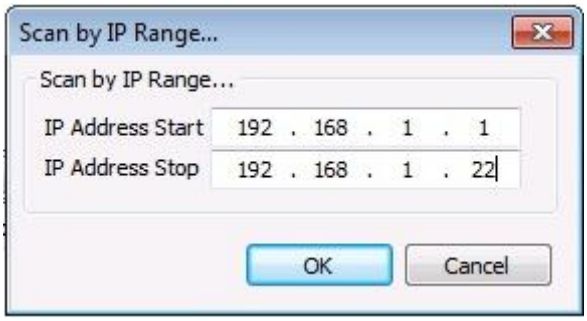
The FEMC presents three different scanning menu options for detecting and enumerating potential F-Response Enterprise target computers.

Scan Network by Domain…(Locates Windows Machines Only)

Scan Network by Domain Dialog

Scan network by domain presents a dialog showing the detected Windows Network Domains and/or Workgroups. Select either an individual domain/workgroup, or the Entire Network.

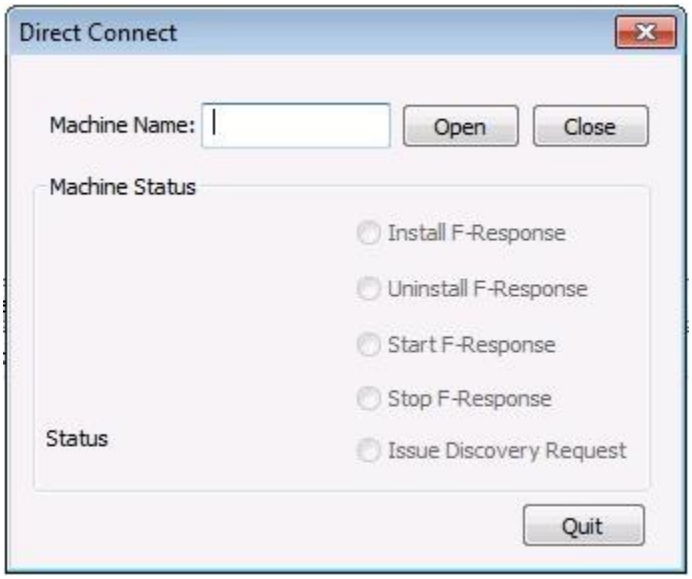
Scan Network by IP Range…(Locates Windows and Unix Machines)



Scan Network by IP Range Dialog

Scan network by IP Range presents a dialog that accepts a start and end IP address (inclusive) for an IP Range to be scanned.

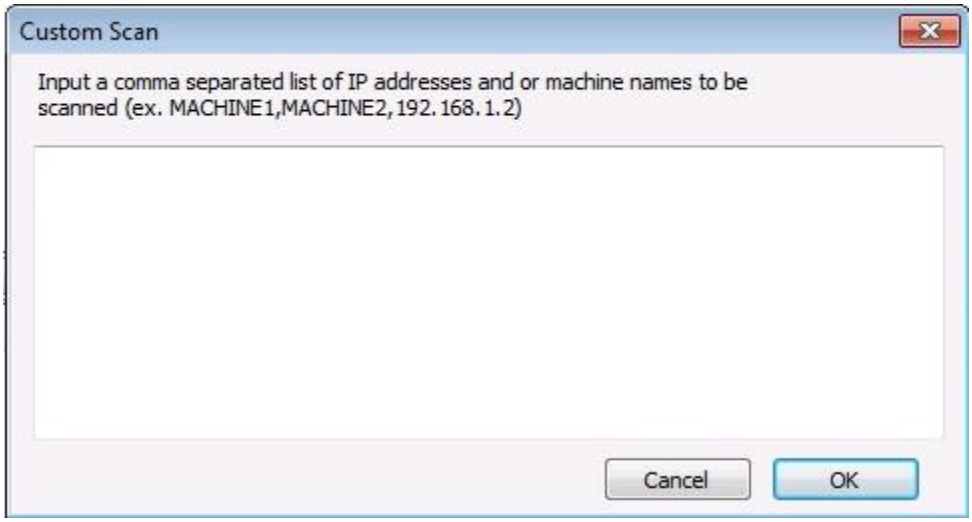
Direct Connect… (Locates Windows and Unix Machines)



Direct Connect Dialog

Direct Connect presents a dialog that accepts a computer Network name or IP Address and attempts to connect to the computer to perform any of the following actions: Install, Uninstall, Start, Stop, and Issue Discovery Request.

Custom Scan… (Locates Windows and Unix Machines)

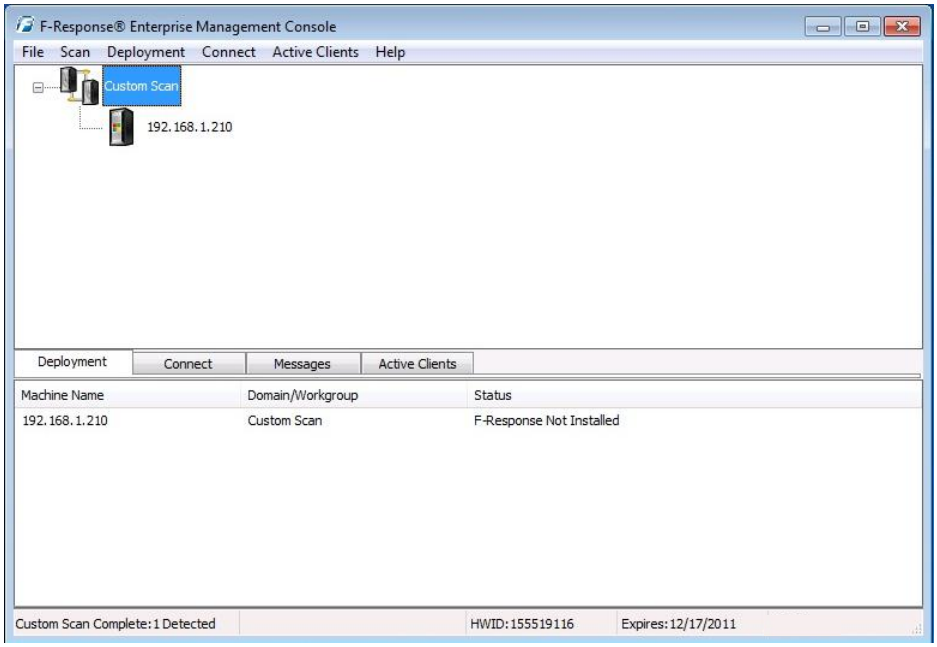

Custom Scan
Input a comma separated list of IP addresses and or machine names to be scanned (ex. MACHINE1,MACHINE2,192.168.1.2)
Cancel
OK

Custom Scan Dialog

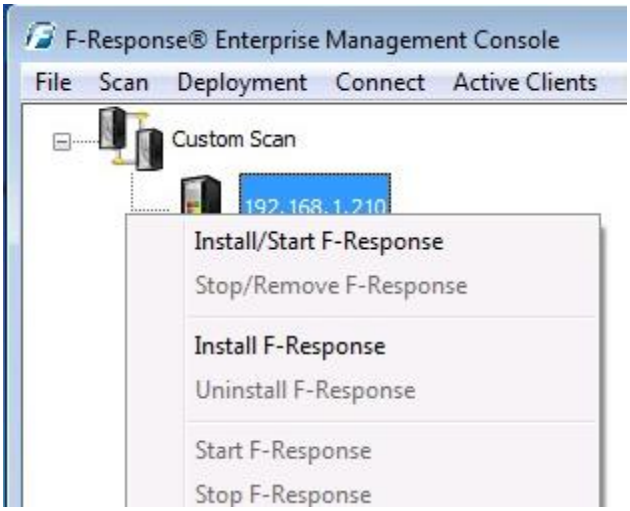
Custom Scan presents a dialog that accepts a comma delineated listing of either computer names or IP addresses (or both) to scan to detect F-Response Enterprise installations and/or potential targets. In addition the Custom Scan dialog will present the last executed scan input on opening.

Enterprise Edition – Deploying and Managing F-Response using the FEMC (All Supported Platforms)

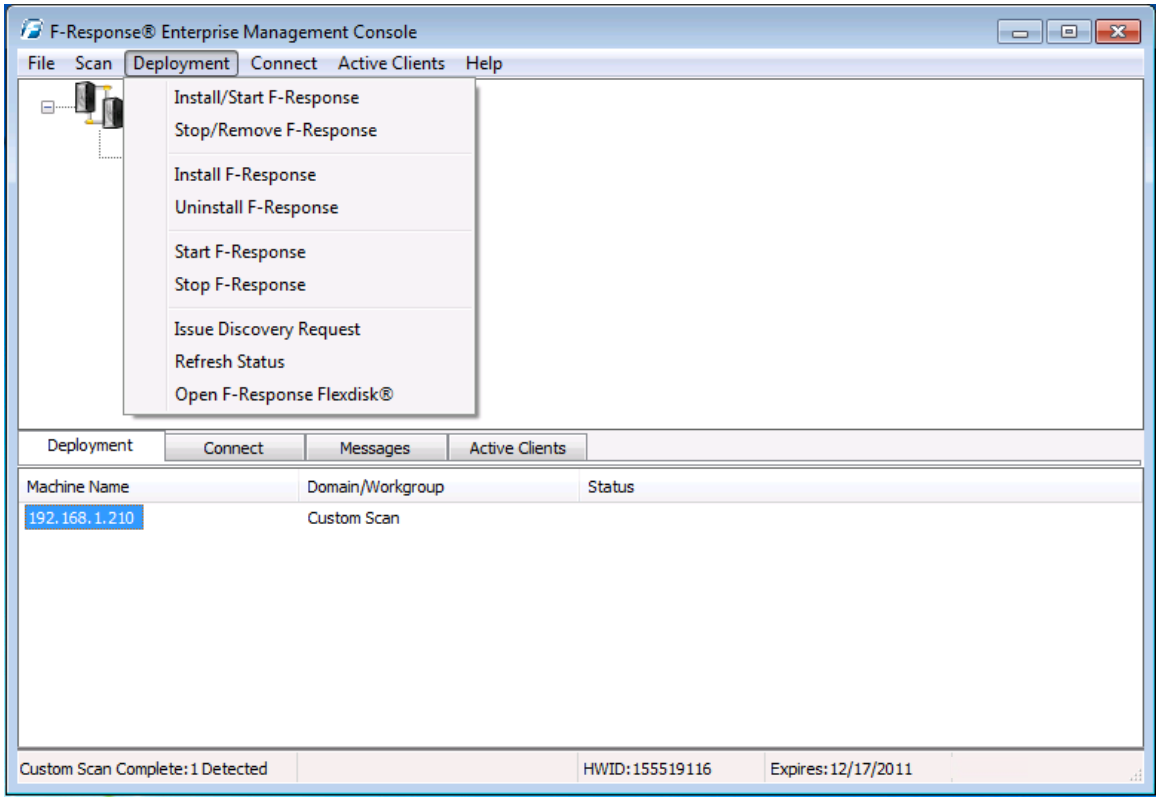
Following a successful scanning/enumeration process, the F-Response Enterprise Management Console can then be used to install, start, stop, and uninstall F-Response Enterprise from accessible computers on the network. The following is a step by step progression for using the FEMC to install, start, connect to, disconnect from, stop, and uninstall F-Response Enterprise on remote computers.



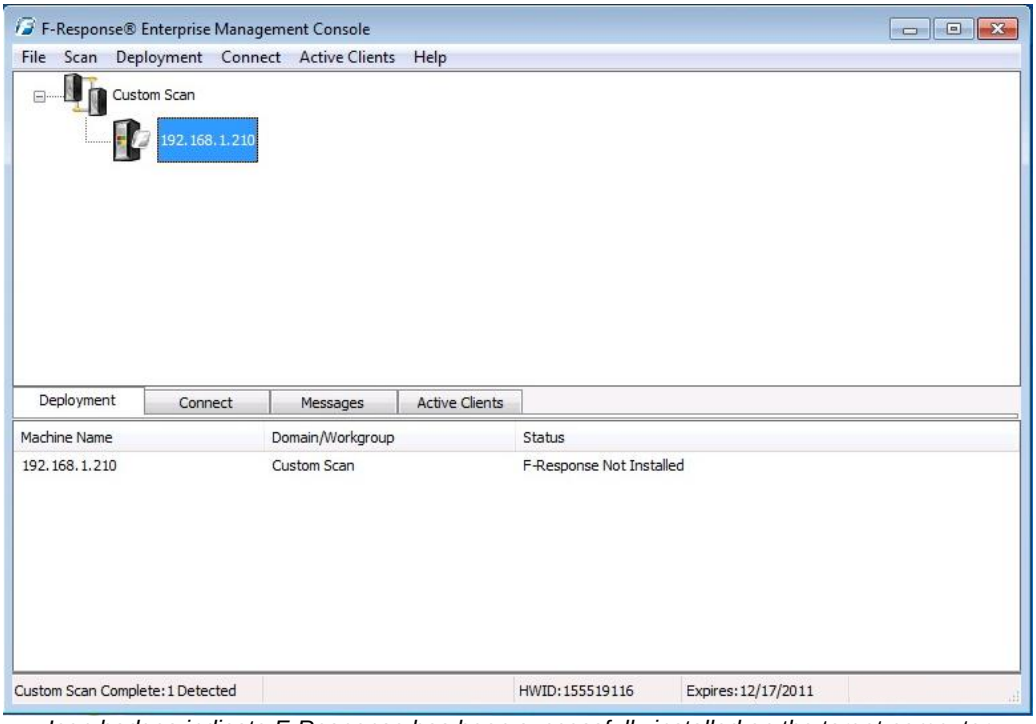
Completed Custom Scan operation, results show one accessible computer. Please see Appendix H for the complete icon legend defining the different platforms.



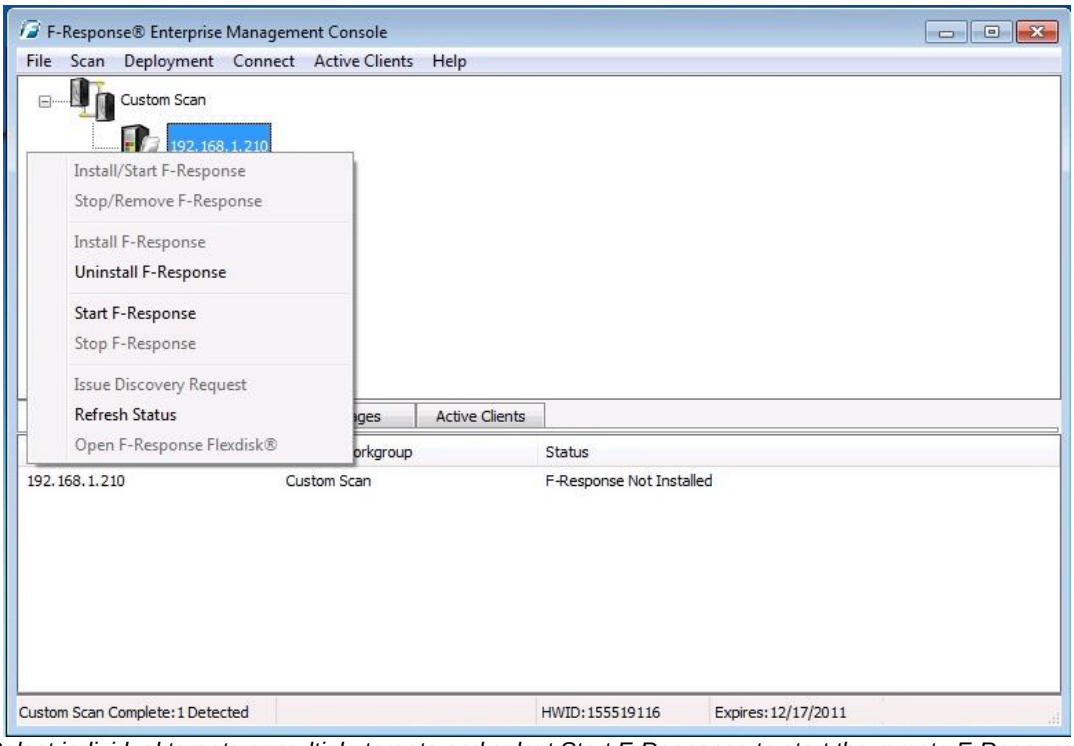
Installation of F-Response can be performed by right-clicking on a valid target icon.



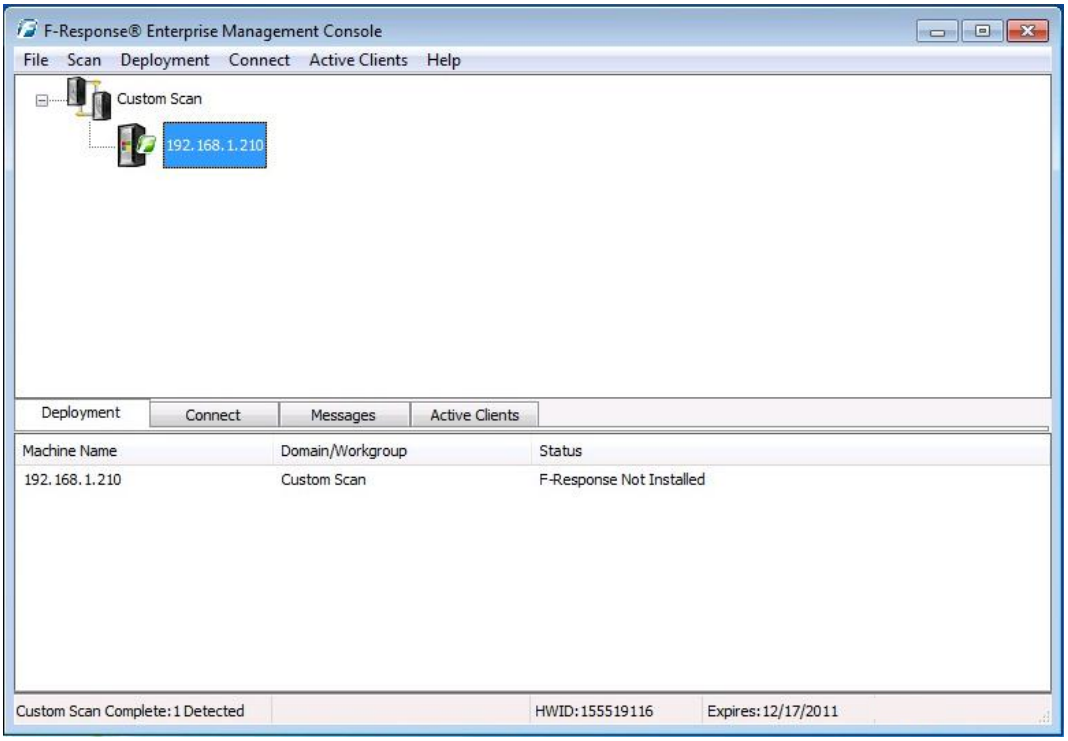
Installation can also be performed on multiple targets by selecting them in the Deployment panel.


F-Response® Enterprise Management Console
File Scan Deployment Connect Active Clients Help
Custom Scan
192.168.1.210
Deployment Connect Messages Active Clients
Machine Name Domain/Workgroup Status
192.168.1.210 Custom Scan F-Response Not Installed
Custom Scan Complete:1 Detected HWID:155519116 Expires:12/17/2011

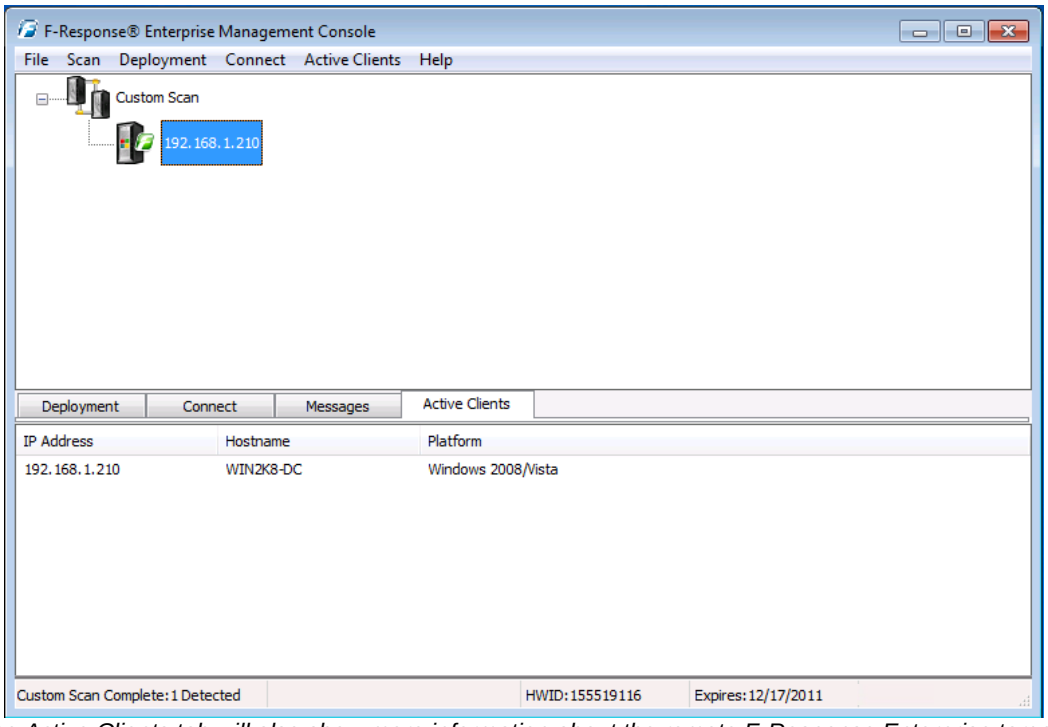
Icon badges indicate F-Response has been successfully installed on the target computer



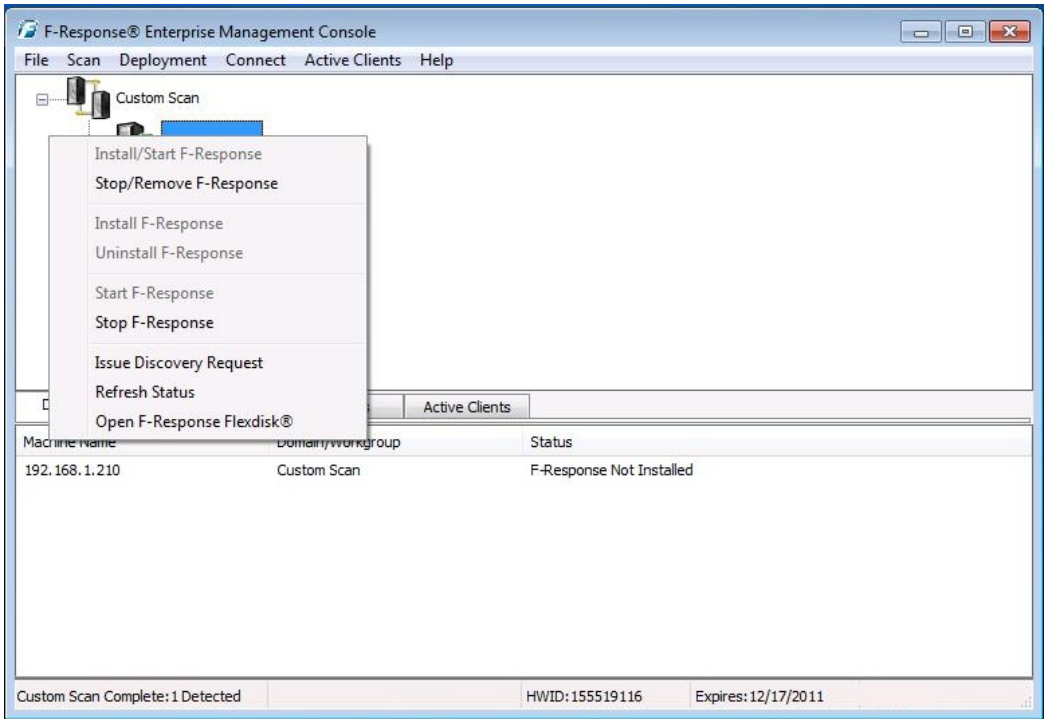
Select individual targets or multiple targets and select Start F-Response to start the remote F-Response Enterprise service.



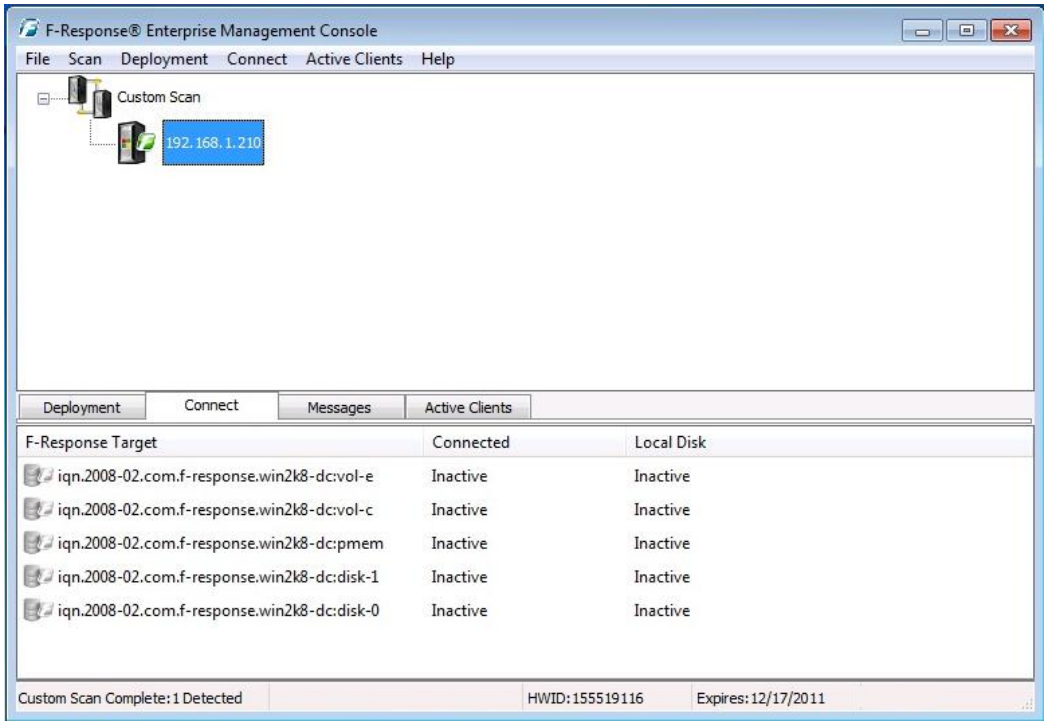
Icon badges indicate F-Response has been successfully started on the target computer



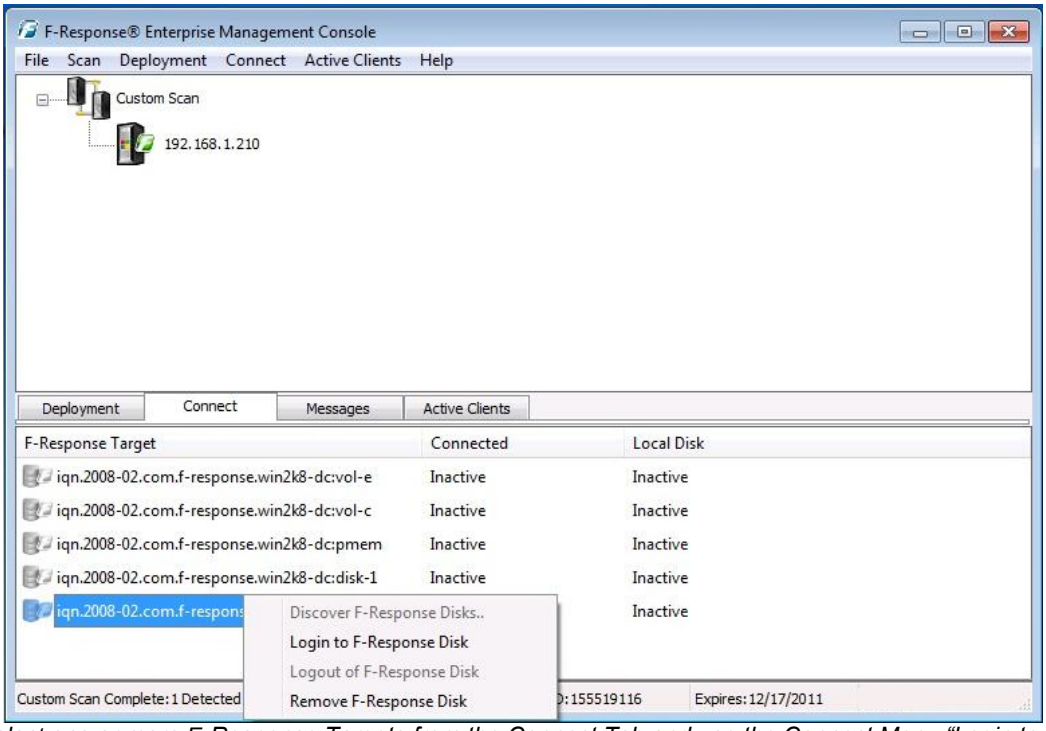
The Active Clients tab will also show more information about the remote F-Response Enterprise targets currently connected to your license dongle, including platform, hostname, and IP Address.



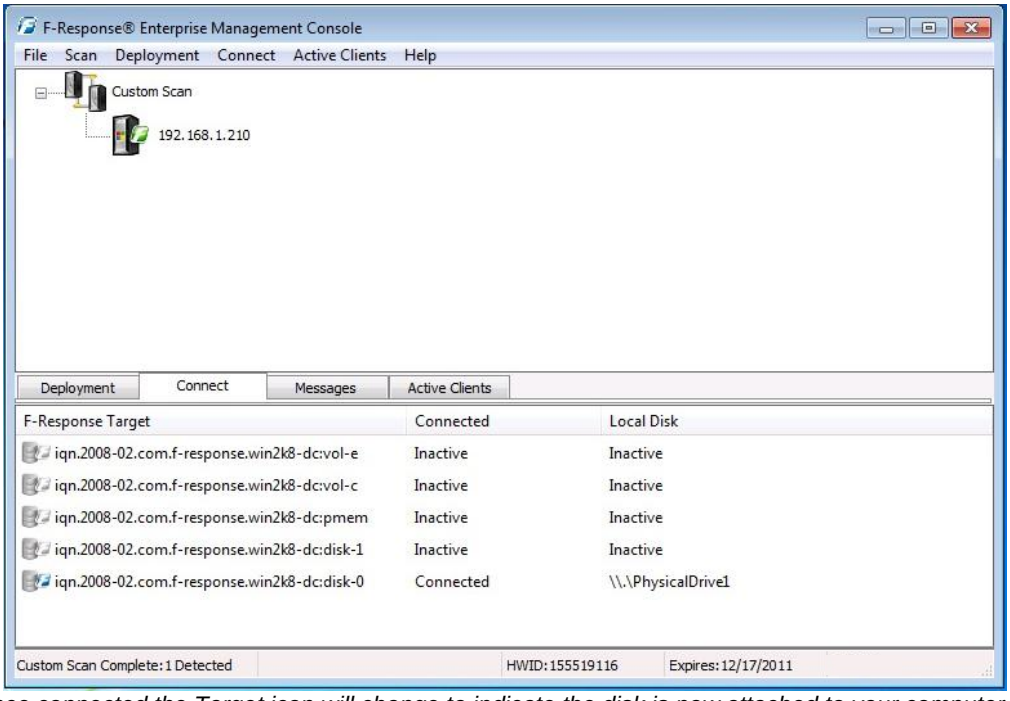
Issue Discovery Request will obtain a complete listing of the available targets from the remote F-Response Enterprise computers.



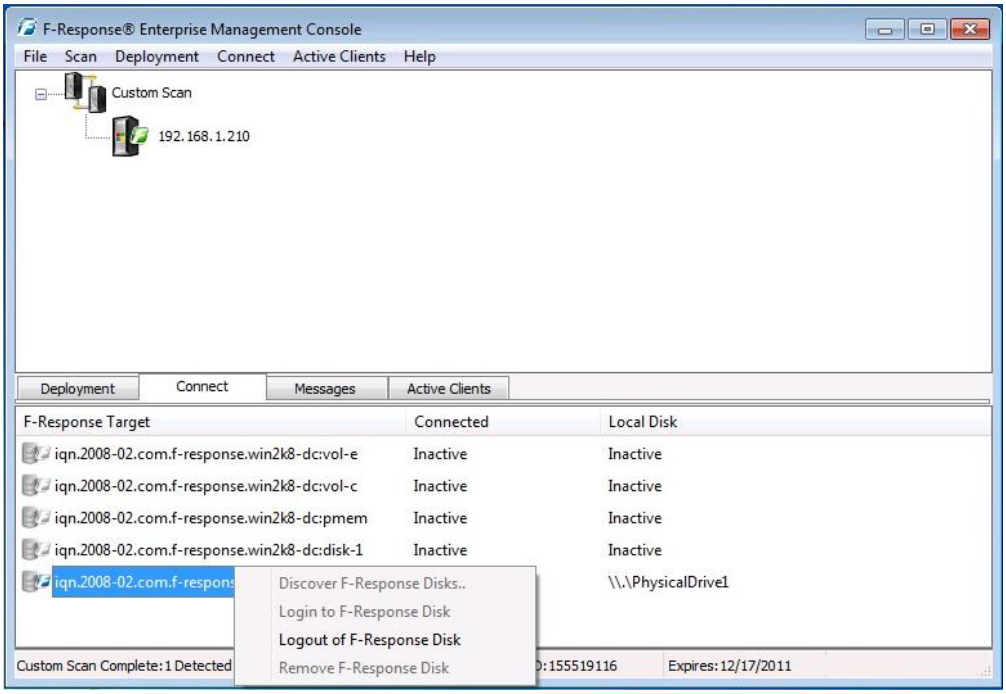
The Connect Tab displays a listing of the accessible disks, logical volumes, and physical memory (if available) for each F-Response Enterprise Target. (For more information on the naming convention used see Appendix G)



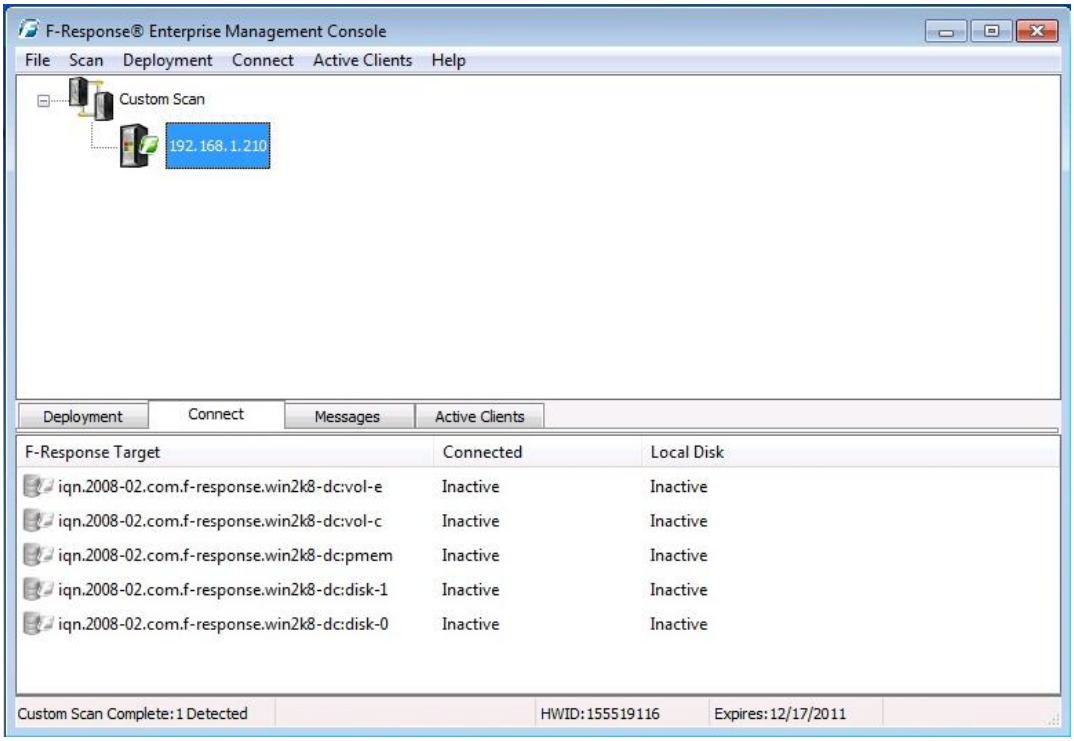
Select one or more F-Response Targets from the Connect Tab and use the Connect Menu "Login to F-Response Disk" to authenticate and login to the remote device.



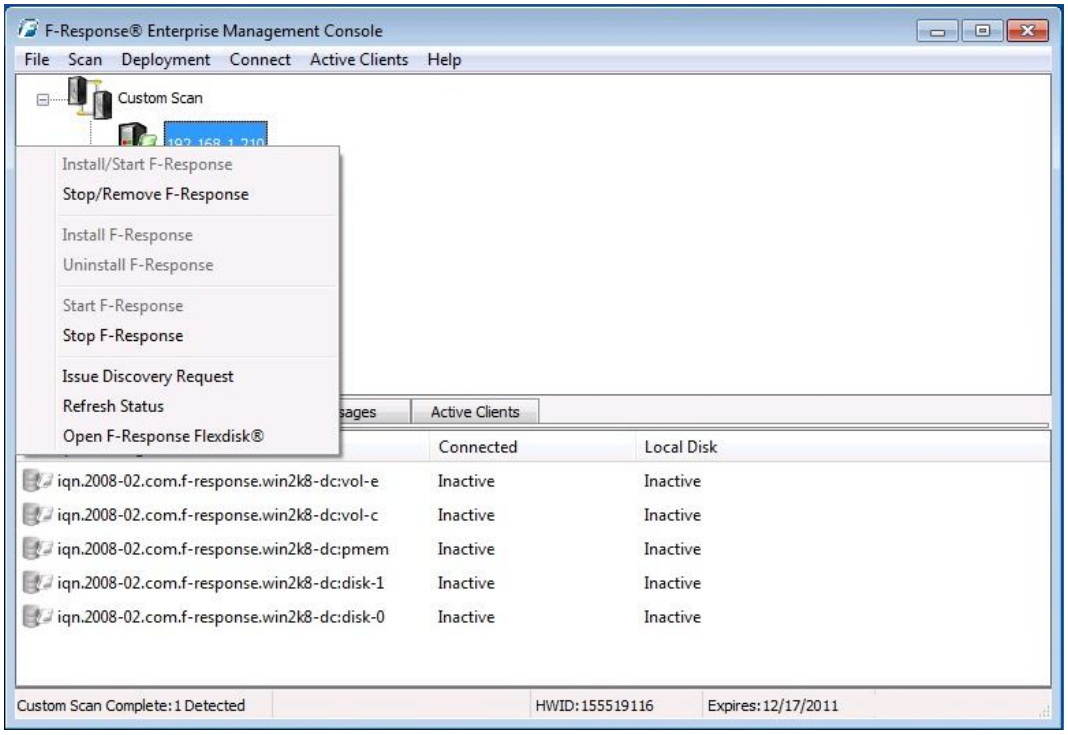
Once connected the Target icon will change to indicate the disk is now attached to your computer, in addition the local mapping information will be provided, in the above instance the Windows disk-0" has been mapped to PhysicalDisk1.



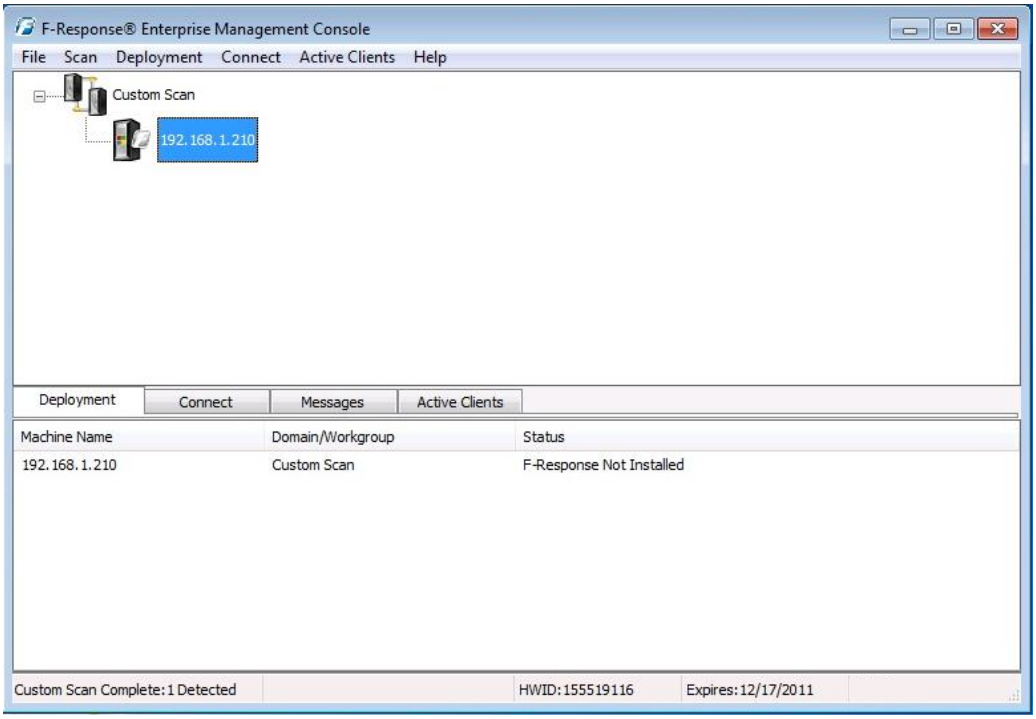
To logoff select one or more connected F-Response Targets and select the Connect Menu "Logout of F-Response Disk" option.



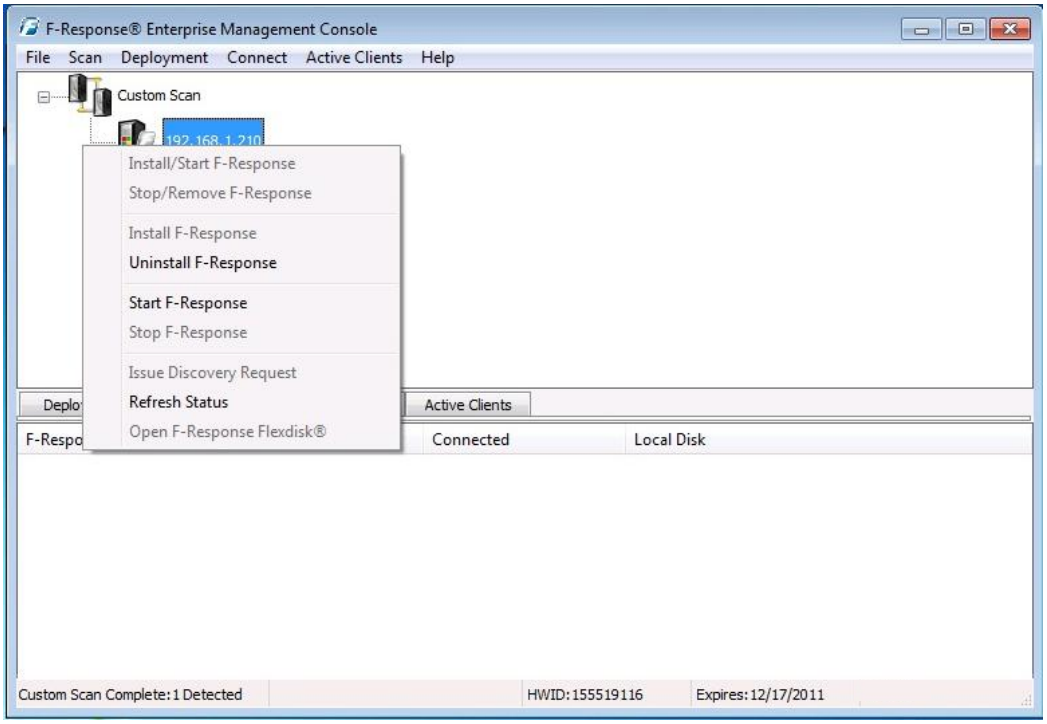
After successful logout the F-Response Target Icon will change and the status indicator becomes Inactive.



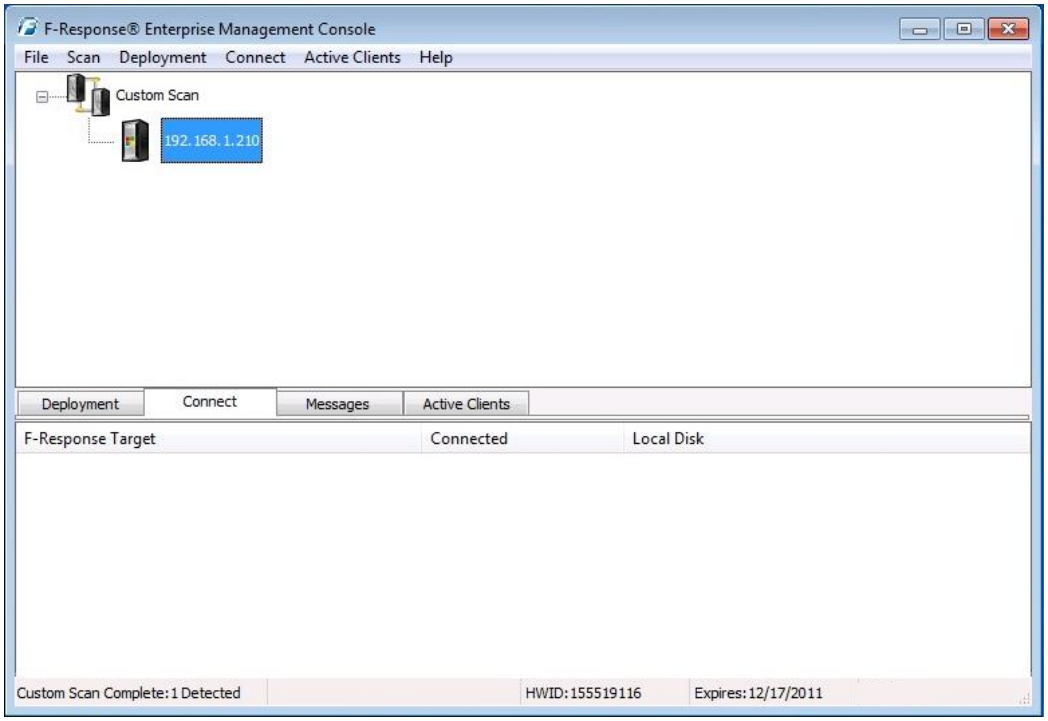
When complete, select individual targets or multiple targets and select Stop F-Response to stop the remote F-Response Enterprise service.



Icon badges indicate F-Response has been successfully stopped on the target computers



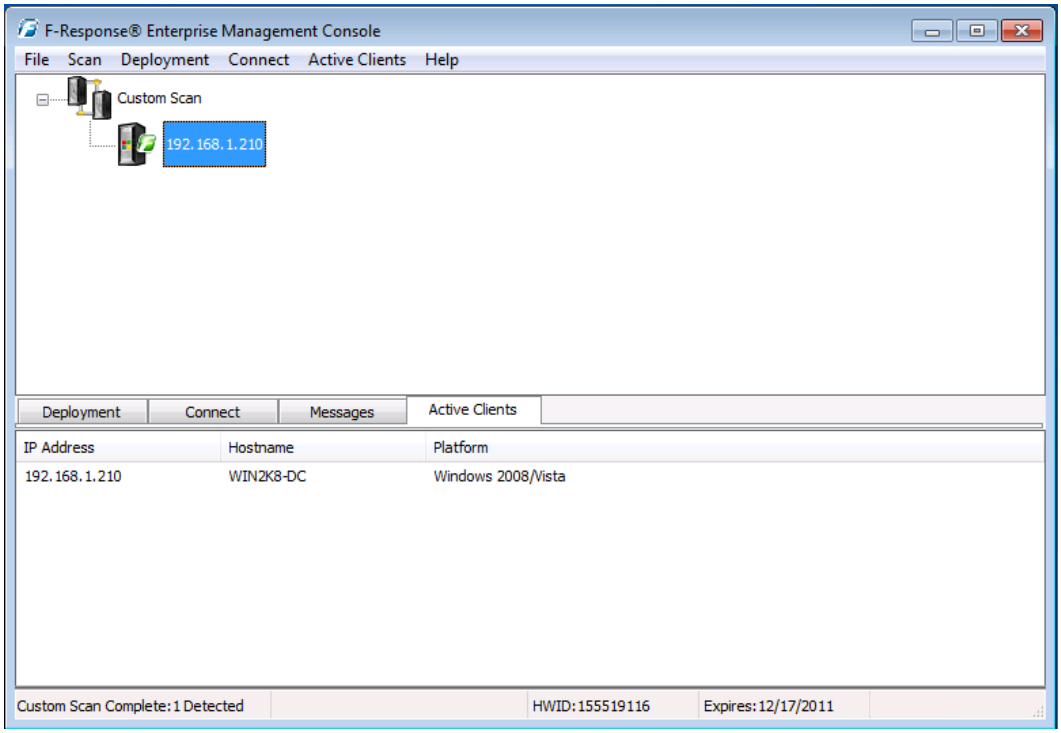
When complete, select individual targets or multiple targets and select Uninstall F-Response to uninstall the remote F-Response Enterprise service.



Icons indicate F-Response has been successfully uninstalled on the target computers

Enterprise Edition – Using F-Response Enterprise Edition for Windows (Deployment without the FEMC)

- **Step 1**
  - To use the F-Response Enterprise Edition, insert a valid F-Response FOB key into a USB port of the computer *on which you will be running the F-Response License Manager Service*, and then execute the F-Response LM Server on this computer.
- **Step 2**
  - Start the remote F-Response Enterprise Service which has been *installed and configured* on the Target computer (See Appendix A for details regarding the command line options for installing, uninstalling, and configuring F-Response Enterprise on each target machine.)
  - Once an F-Response Enterprise Edition target has been successfully validated, the F-Response Enterprise Management Console Active Clients Tab will show the remote client's IP address, Machine name, and Platform as shown below. Clients listed under the Active Clients tab are available for F-Response connections using the F-Response FEMC, Accelerator, or iSCSI Initiator.



F-Response Enterprise Management Console Active Clients Tab

To examine multiple targets, simply start the remote F-Response Enterprise Service on each Target.

To see the available targets on the remote computer select the IP address in the Active Clients panel and use the context menu option "Issue Discovery Request".

F-Response Consultant + Covert Edition

Consultant + Covert Edition – Overview

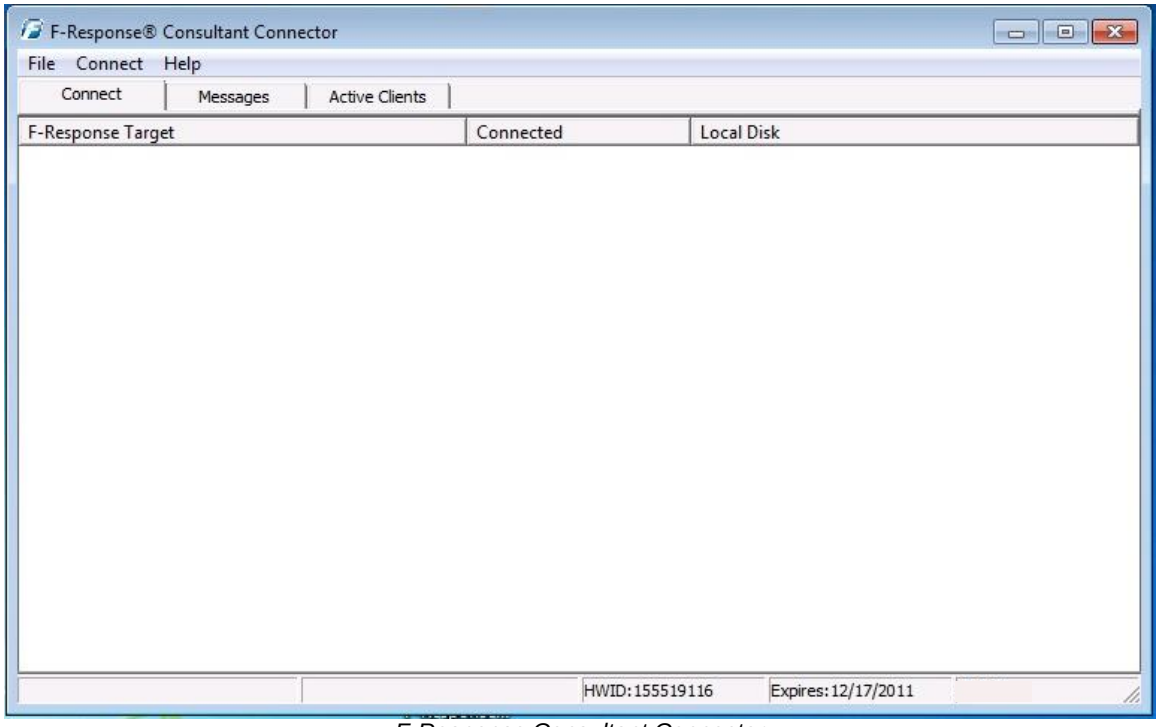
The Consultant + Covert Edition provides all the capabilities of the F-Response Consultant Edition (see the following F-Response Consultant Edition section of this document), however it additionally provides a limited covert deployment console capable of deploying and starting F-Response on a single active target.

Please refer to the following sections to learn more about configuring the F-Response Consultant + Covert Console:

- F-Response Enterprise Configuring Deployment Options
- F-Response Enterprise Configuring Credentials
- F-Response Enterprise Scanning (Direct Connect Only)

F-Response Consultant Edition

Consultant Edition – Overview of the F-Response Consultant Connector



F-Response Consultant Connector

Menu Options

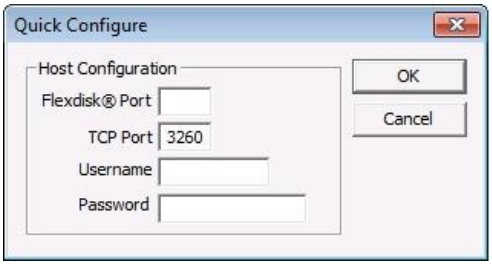
- File
  - Quick Configure…:
    - Opens a dialog to configure the TCP Port, Username, and Password for use during Discovery Request or Login phases.
  - Create Autoconfigure…:
    - Opens a dialog for creation of an Autoconfigure package for F-Response Consultant Edition.
  - Clear Messages:
    - Clears any information or error messages currently in the Messages Panel.
  - Exit:
    - Close and exit the F-Response CC console.
- Connect
  - Discovery F-Response Disks…
    - Opens a dialog providing iSCSI Discovery request capability by IP Address.
  - Login to F-Response Disk

        - Initiates a iSCSI login on the selected F-Response Consultant Target.
    - Logout of F-Response Disk
        - Initiates a iSCSI logout on the selected F-Response Consultant Target.
    - Remove F-Response Disk
        - Deletes all F-Response Disks for the selected target from the Connect Tab.
    - Open F-Response Flexdisk™
        - Opens the default configured web browser pre-populated to connect to the Flexdisk™ target.
- Help
    - About
        - Presents a splash screen indicating the version information of the F-Response Consultant Connector Console (FCC).

Tab Controls

- Connect
    - Displays a listing of the F-Response Target(s) after a successful Discovery Request.
- Messages
    - Displays informational Messages during operation, if errors occur they will be noted here.
- Active Clients
    - Queries the F-Response License Manager Service to obtain active clients for the F-Response LM dongle. This list includes IP Address, Network Name, and Platform.

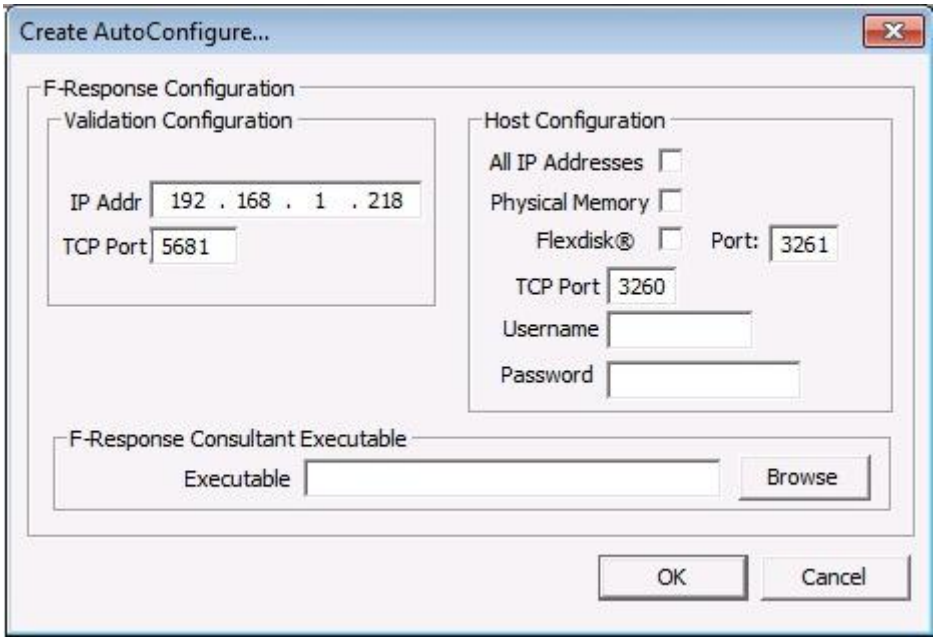
Consultant Edition – Configuring the FCC Console (Quick Configure)



The Quick Configure dialog allows you to quickly configure the port, username, and password value for the F-Response connection.

- Host Configuration
  - Flexdisk™ Port
    - The TCP Port the remote F-Response Consultant edition is listening on for incoming Flexdisk™ (HTTPS) connections.
  - TCP Port
    - The TCP Port the remote F-Response Consultant edition is listening on for incoming F-Response connections.
  - Username
    - The Username configured on the remote F-Response Consultant edition target.
  - Password
    - The Password configured on the remote F-Response Consultant edition target.

Consultant Edition – Configuring the FCC Console (Create AutoConfigure)



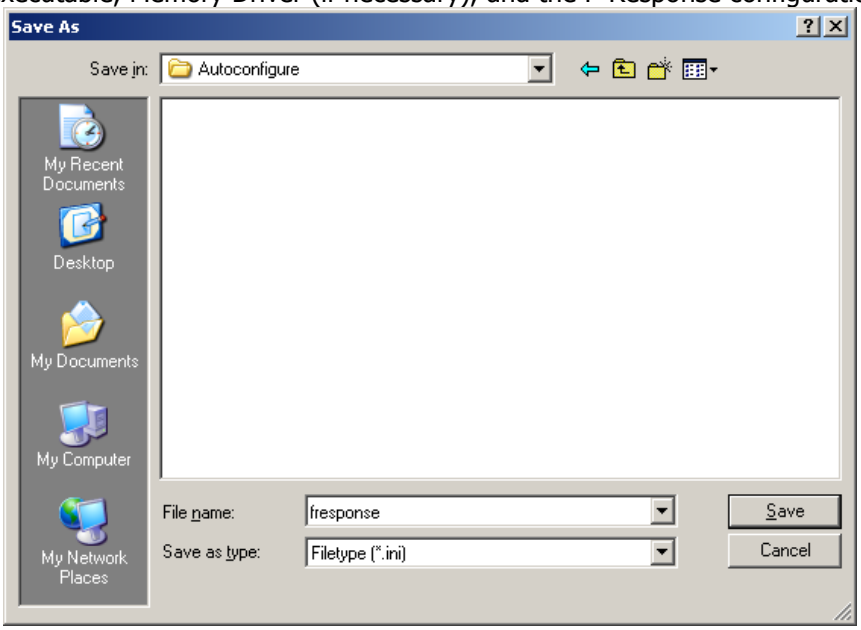
The Create Autoconfigure dialog allows you to create an Autoconfigure package which when executed on the remote machine will bring up F-Response completely pre-configured and ready to start.

- F-Response Configuration
  - Validation Configuration
    - IP Addr:
      - Configures the IP Address of the F-Response LM Service.
    - TCP Port:
      - Configures the TCP Port of the F-Response LM Service.
  - Host Configuration
    - All IP Addresses
      - Check to enable automatic binding to all IP Addresses.
    - Physical Memory
      - Check to enable Physical Memory access on the remote F-Response Target (Supports Windows clients only).
    - Flexdisk™ Port
      - TCP Port the remote F-Response Consultant executable should listen on for Flexdisk™(HTTPS) connections.
    - TCP Port
      - TCP Port the remote F-Response Consultant executable should listen on for login and discovery requests.
    - Username
      - The Username the remote F-Response Consultant executable should use for login and discovery requests.
    - Password

- The Password the remote F-Response Consultant executable should use for login and discovery requests.

- F-Response Consultant Executable:
  - Executable
    - Use the browse button to locate the F-Response Enterprise executable to install (Typically located in C:\Program Files\F-Response\F-Response Consultant Edition\).

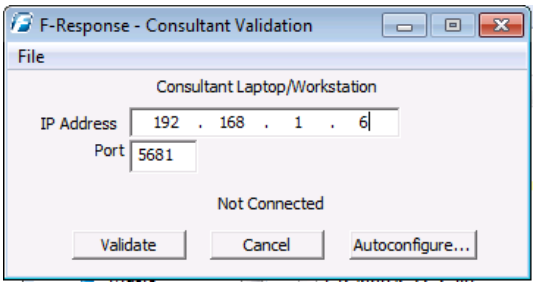
Pressing OK opens the file save dialog allowing you to select a destination for the F-Response Consultant executable, Memory Driver (if necessary), and the F-Response configuration file.



Save the Autoconfigure "package" to a usb disk or portable storage device so that it can be taken to the target computer for execution.

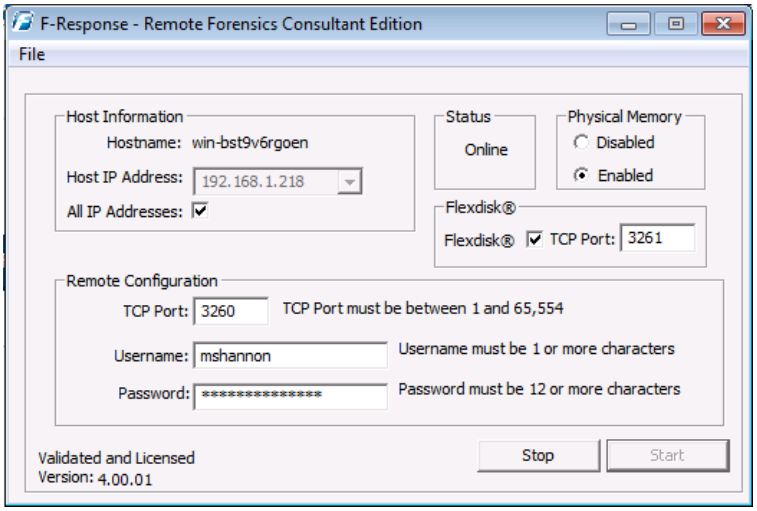
Consultant Edition – Using F-Response Consultant Edition for Windows

- **Step 1**
  - To use the F-Response Consultant Edition, insert a valid F-Response FOB key into a USB port of the computer *on which you will be running the F-Response License Manager Service*, and then execute the F-Response License Manager Service on that computer.
- **Step 2**
  - If you are using the "Autoconfigure" feature unique to the Consultant Edition, jump to Step 7.
  - If you are not using the "Autoconfigure" feature, make the F-Response CE Target code available to the machine *to be analyzed* (via USB, network share, CD, etc.,) and execute the F-Response CE Target code. The following consultant validation box will appear.



F-Response Consultant Edition Validation User Interface (See Appendix A for field information detail)

  - Enter the IP address of the computer running the F-Response License Manager service (in this case our F-Response LM server is listening on port 5681 at address 192.168.1.6), and select "validate". The following appears, albeit with the fields empty, if a valid license key is found:



F-Response User Interface, configured for use. (See Appendix B for field information detail)

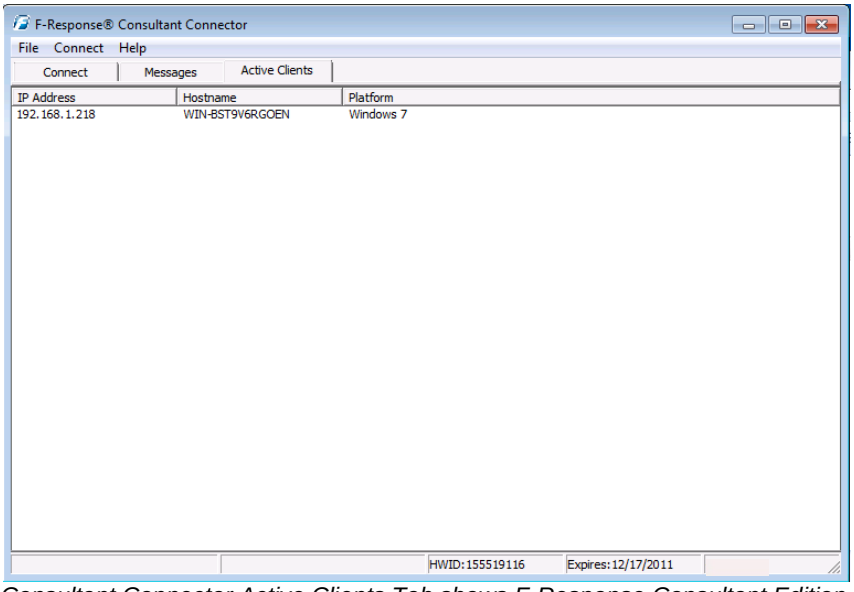
- **Step 3**
  - Select an IP Address from the "Host IP Address" drop-down arrow to bind the F-Response Target code to a local IP address currently in use by the computer. In this case we have chosen 192.168.1.218.
  - Alternatively you can select "All IP Addresses" to bind to all available IP addresses.

- **Step 4**
  - Select the TCP Port. In this instance we chose to keep the default '3260'.
  - [OPTIONAL] Select the Flexdisk™ Port. In this instance we chose to keep the default "3261".

- **Step 5**
  - Enter in a username and password value. These values will be used later to authenticate the network connection to this computer.

- **Step 6**
  - Press the "Start" button to start listening for incoming connections.
  - When the service is started one temporary file is created if the Physical Memory option has been enabled. This file "Mnemosyne.sys" is the physical memory driver necessary for providing access to physical memory.

  - At this time, the F-Response Consultant Edition client has been successfully validated, and the F-Response Consultant Connector Active Clients Tab shows the remote client's IP address, Machine name, and Platform as shown below.



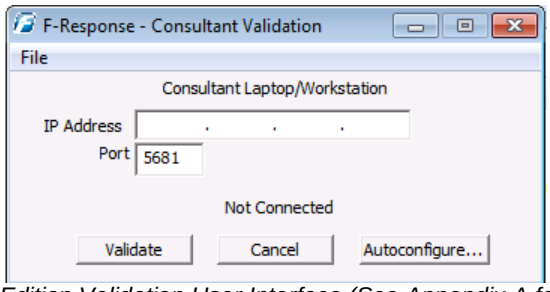
F-Response Consultant Connector Active Clients Tab shows F-Response Consultant Edition remote client or target computer.

The Consultant Edition permits you to establish multiple connections. To examine multiple targets, simply start the remote F-Response Consultant Service on each Target and they will each appear in the F-Response Consultant Connector Active Clients Tab.

This completes F-Response preparation for this session. Remember – **you will need the four entries selected in the User Interface from Step 2 above in order to establish the connection to access the computer's drives over the network.** Refer to the section on using the F-Response Consultant Connector to complete the connection(s) and access the local machine's physical drives from remote.

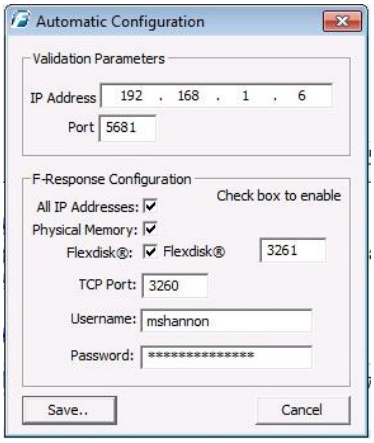
Steps 7 through 10, below, are applicable only if you are using the "Autoconfigure" feature unique to the Consultant Edition. The "Autoconfigure" feature unique to the F-Response Consultant Edition allows you to create a configuration file prior to running F-Response target code on any number of machines to be analyzed. This can be a valuable time saving feature if numerous machines are to be investigated, or if an assistant is going to be starting the tool on a remote machine for the benefit of the examiner. E.g., The examiner can prepare an Autoconfiguration CD-ROM. When analysis is to be conducted, the CD is simply placed in the machine to be analyzed and F-Response is run and started from the CD. No further setup is required.

- **Step 7**
  - Execute the F-Response CE Target code on a suitable machine in order to create the portable configuration files to be used later on the machine(s) to be analyzed. The following consultant validation box will appear.



F-Response Consultant Edition Validation User Interface (See Appendix A for field information detail)

  - Select "Autoconfigure". The following box will appear.

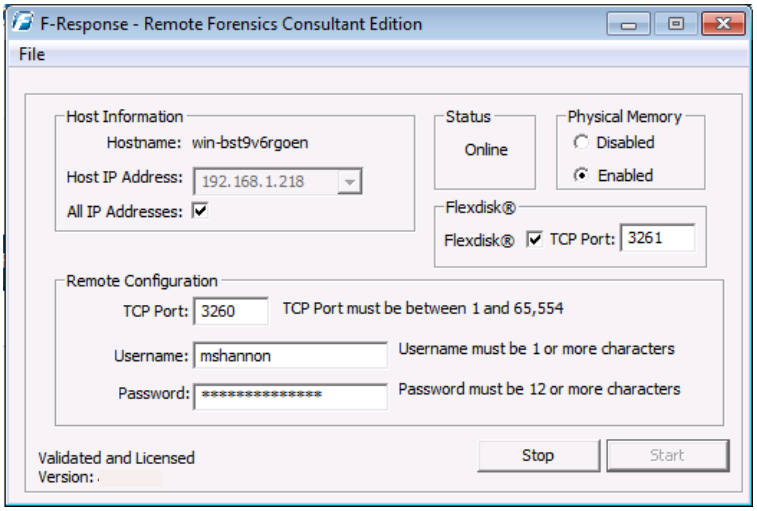


F-Response Consultant Edition Automatic Configuration Option

- In the Validation Parameters section, enter the IP address and Port of the computer running the F-Response License Manager service (in this case our F-Response LM server is listening on port 5681 at address 192.168.1.6).
- In the F-Response Configuration section, enter the iSCSI TCP Port (in this instance we chose to keep the default '3260'), [OPTIONAL] enter the Flexdisk™ TCP Port (in this instance we chose to keep the default '3261'), username (one or more characters), and password value (a minimum of 12 characters). These values will be used later to authenticate the iSCSI/Flexdisk™ network connection to this computer.

- **Step 8**
  - Press the "Save" button to create the automatic Configuration files that will be used on any number of machines to be analyzed.
  - Three files are created; fresponse.ini, flexdmgr.dll (if Flexdisk™ is enabled), and Mnemosyne.sys (if Physical Memory is Enabled).
  - At this time, the F-Response Consultant Edition Automatic Configuration is complete.
  - The examiner can prepare an Autoconfiguration CD-ROM, thumb drive, or other delivery mechanism using the three files shown above; i.e. 1) f-response-ce.exe, 2) fresponse.ini, 3) Mnemosyne.sys (if Physical Memory is enabled), 4) flexdmgr.dll (if Flexdisk™ is enabled).

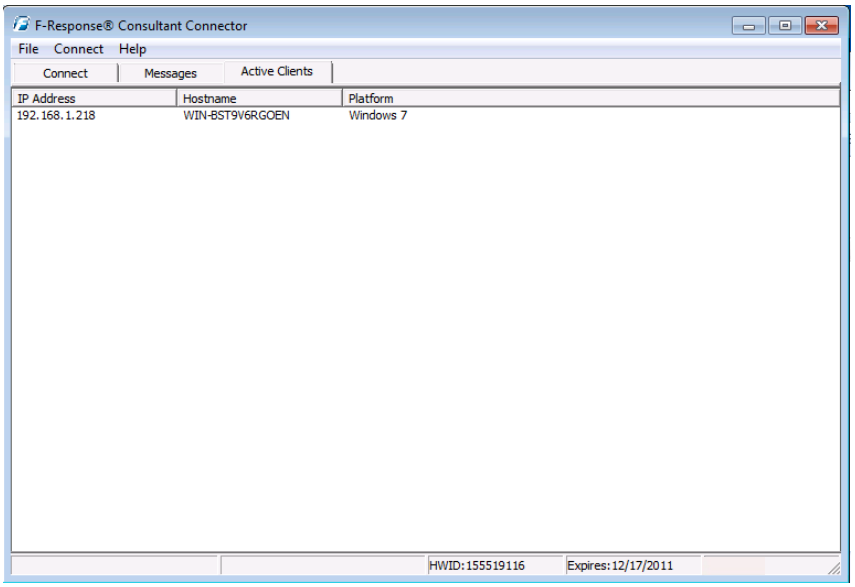
- **Step 9**
  - When analysis is to be conducted, these three files are simply placed in/on the machine to be analyzed. Run "f-response-ce.exe" and the following appears if a valid license key is found:



F-Response User Interface, configured for use. (See Appendix B for field information detail)

  - All of the fields are pre-populated since the configuration has already been auto configured. In some cases, the examiner may have an option to select a different IP Address from the "Host IP Address" drop-down arrow to bind the F-Response Target code to one of multiple local IP addresses in use by the computer. In this case we have chosen to use the default 192.168.1.218.

- **Step 10**
  - Press the "Start" button to start listening for incoming connections.
  - At this time, the F-Response Consultant Edition client has been successfully validated, and the F-Response Consultant Connector Active Clients Tab shows the remote client's IP address, Machine name, and Platform as shown in the following figure:



F-Response Consultant Connector Active Clients Tab shows F-Response Consultant Edition remote client or target computer.

Repeat steps 9 & 10 to make additional machines available for analysis. Each will appear in the F-Response Consultant Connector Active Clients Tab.

Consultant Edition – Using F-Response Consultant Edition for Unix based Targets

```
F-Response Consultant/Enterprise (<PLATFORM>),(Version 4.00.03)
Usage:
  -h                              This help page.
  -a </path/to/devices>           Path to additional devices (Comma
separated, ex /dev/md0,/dev/md1)
  -S <F-ResponseLM IP>            IP Address of F-Response LM Server
  -P <F-ResponseLM Port>          TCP Port of F-Response LM Server, optional,
defaults to 5681
  -u <username>                   F-Response username, must be 8 characters
  -p <password>                   F-Response password, must be 14 characters
  -i <iSCSI Port>                 iSCSI Port, optional, defaults to 3260
  -c <path/to/fresponse.ini>      Optional autoconfigure path, if used no
other commandline options are required
  -f <Flexdisk Port>              Optional Flexdisk port, if not provided
Flexdisk services will not be enabled.

F-Response Consultant/Enteprise Edition can either be run directly from the
commandline (using the various arguments indicated above, or it can be run
with the -c <path/to/fresponse.ini> option provided the path points to a
valid fresponse.ini file. See the F-Response Consultant Connector
autoconfigure option to generate a valid "fresponse.ini"
```

F-Response command line help on analyst machine

The F-Response Consultant Edition target code for non-Windows platforms is installed and available in the C:\Program Files\F-Response\F-Response Consultant Edition\ folder. The executable name will indicate which version is appropriate for your target platform.

Platform	**F-Response Target Code**
Linux (glibc 2.3.5+) Intel/i386	f-response-ce-e-lin
Linux (glibc 2.3.5+) x64	f-response-ce-e-lin-64
Apple OSX (10.3, 10.4, 10.5, 10.6, 10.7, 10.8) Universal Binary	f-response-ce-e-osx
Sun Solaris (8,9,10) SPARC	f-response-ce-e-sun
Oracle Solaris/OpenSolaris Intel	f-response-ce-e-sun-i386
IBM AIX (5.1,5.2,5.3,6.1) Power 5	f-response-ce-e-aix-p5
IBM AIX (5.1,5.2,5.3,6.1) Power 6	f-response-ce-e-aix-p6
HP Unix (11iv2,11iv3) Itanium	f-response-ce-e-hpux
FreeBSD (7) Intel/i386	f-response-ce-e-fbsd
FreeBSD (7,8) x64 Intel	f-response-ce-e-fbsd-64
SCO Unix (Open Server 6, Unixware 7) Intel/i386	f-response-ce-e-sco
Google Android(ARM)	f-response-ce-e-android-arm
NetGear ReadyNAS (SPARC)	f-response-ce-e-readynas-sparc

Example Usage:

Scenario #1 – The F-Response target platform is Linux and the F-Response License Manager Server is on 192.168.1.6, Port 5681

Make the F-Response CE Target code available to the machine *to be analyzed* (via USB, network share, CD, etc.)

Execute the F-Response Target code on the machine as "Root", please see "Appendix E – Understanding Unix Credentials" for more information.
At the command line on the target platform type:

```
./f-response-ce-e-lin –S 192.168.1.6 –P 5681 –u <FRESUSERNAME> –p
<FRESPASSWORD> –i 3260
```

Scenario #2 –Using the F-Response Autconfigure file "fresponse.ini" created using F-Response Consultant Connector. The F-Response target platform is Linux.

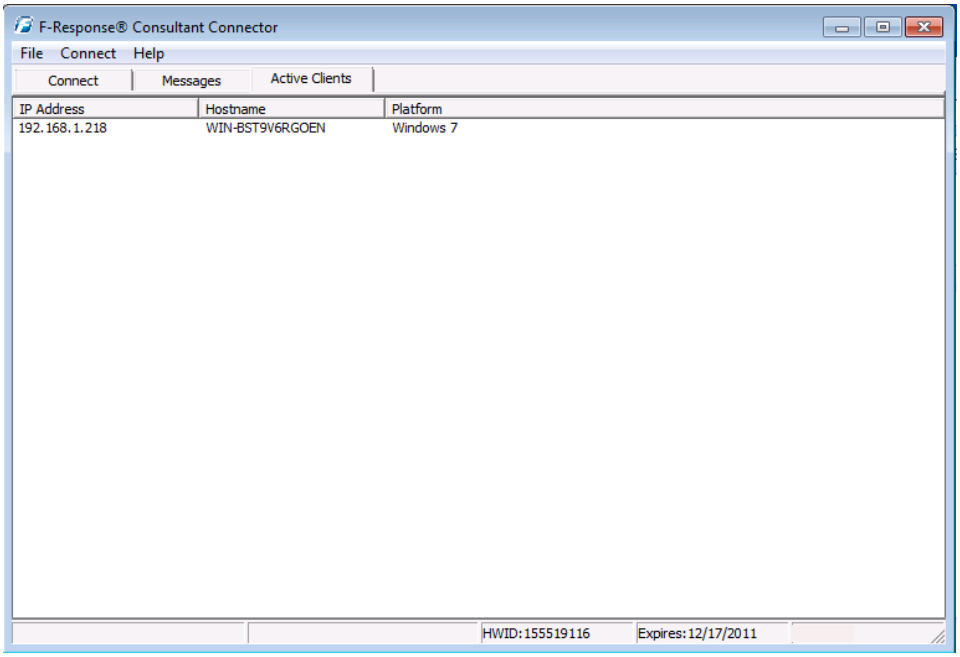
Make the F-Response CE Target code and the "f-response.ini" created by the Consultant Connector available to the machine *to be analyzed* (via USB, network share, CD, etc.)

Execute the F-Response Target code on the machine as "Root", please see "Appendix E – Understanding Unix Credentials" for more information.

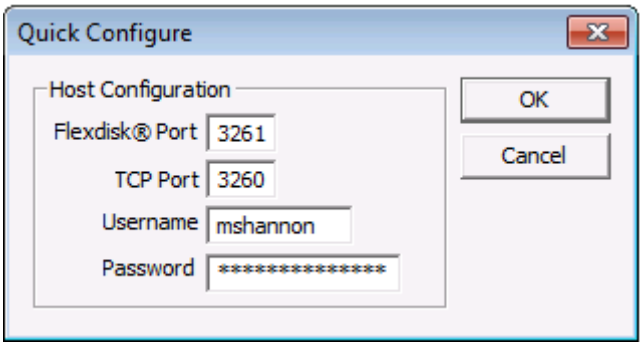
At the command line on the target platform type:

```
./f-response-ce-e-lin –c fresponse.ini
```

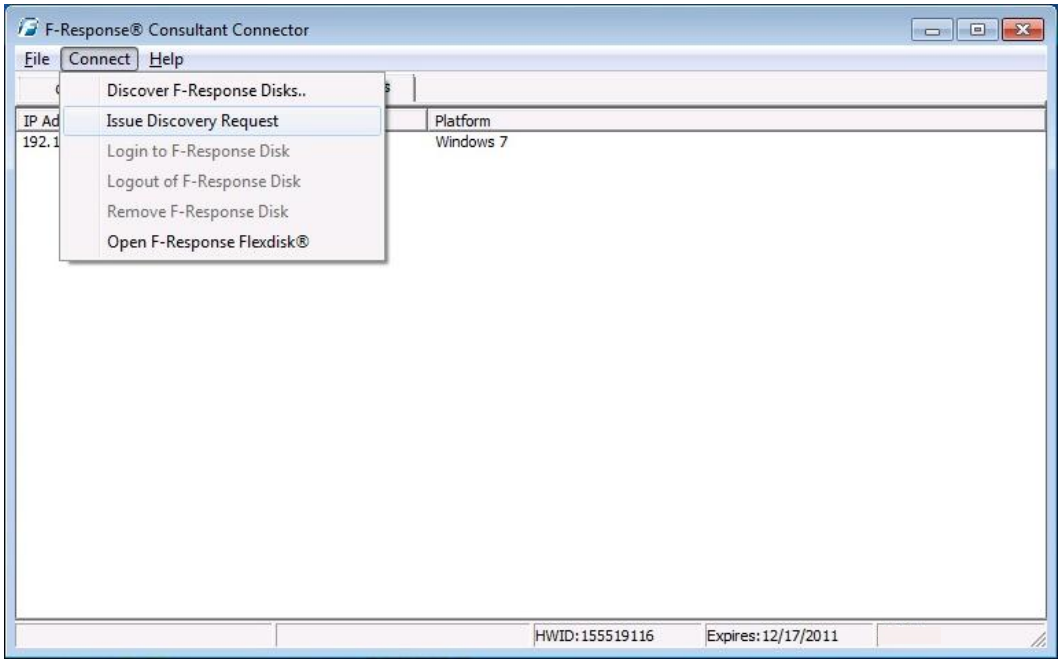
Consultant Edition – Using the F-Response Consultant Connector



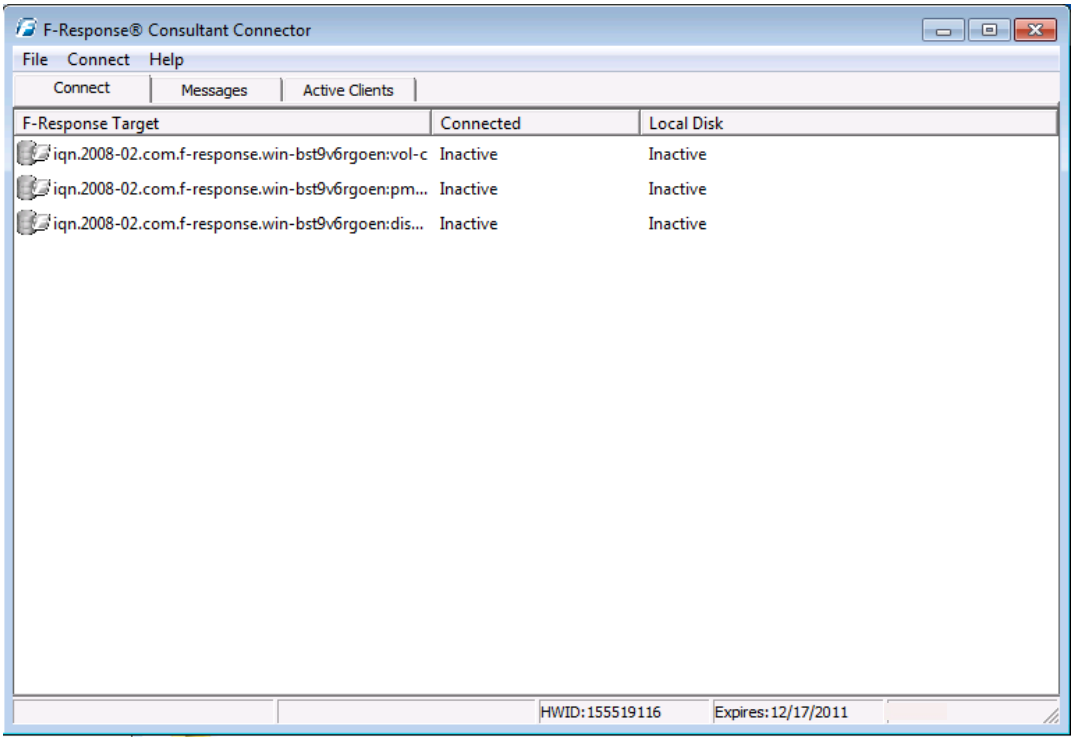
The Active Clients Tab in the F-Response Consultant Connector shows clients actively connected to the F-Response License Manager.



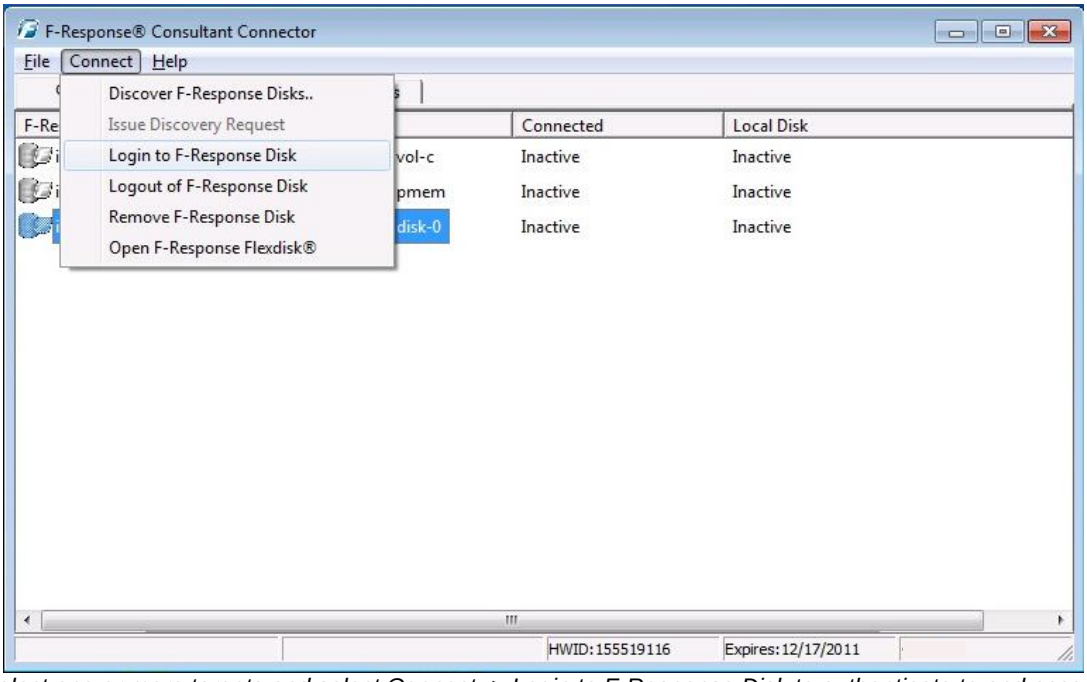
Prior to issuing a Discovery Request or Connecting to an F-Response Target you must first input your username and password information into either the File->Quick Configure or Create Autoconfigure Dialog, these are the same username and password values entered on the Consultant remote target gui.



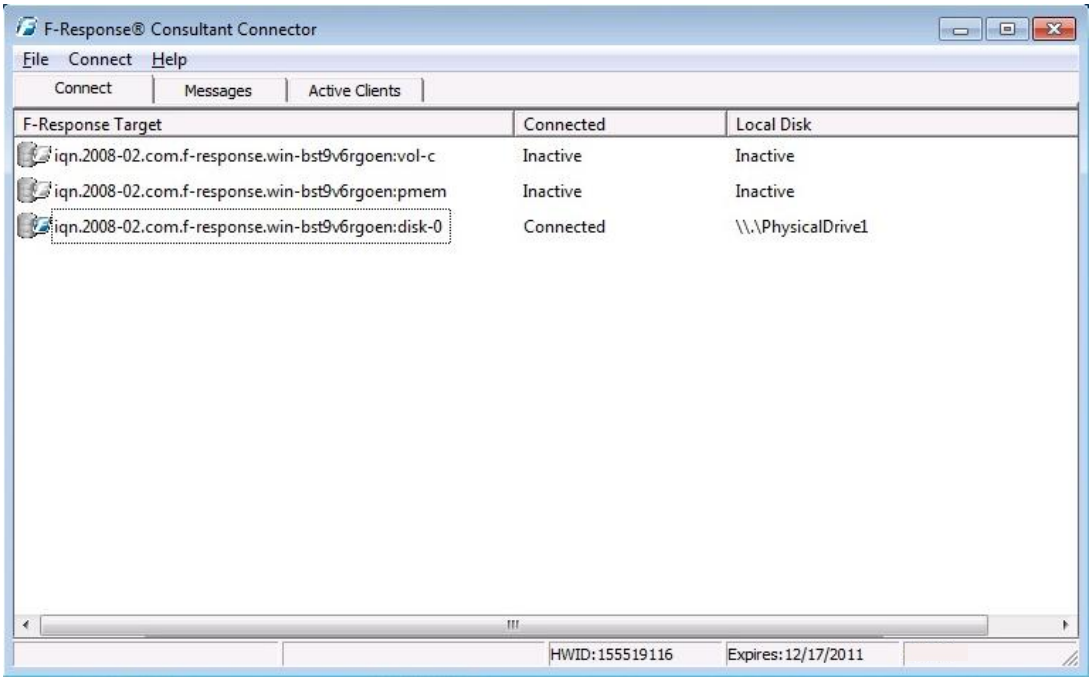
Select one or more Active Clients and select Connect->Issue Discovery Request to perform a discovery request against the remote target.



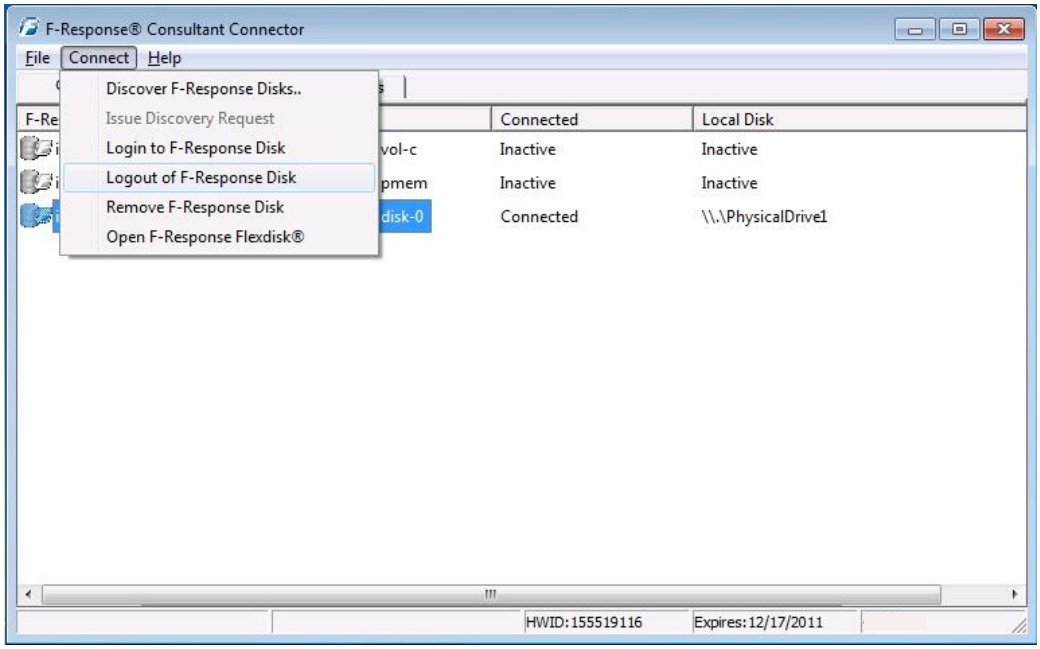
Following a successful Discovery Request the Connect Tab will contain a listing of valid Targets (Physical Disks, Logical Volumes, and/or Physical Memory). More on Target naming in Appendix G.



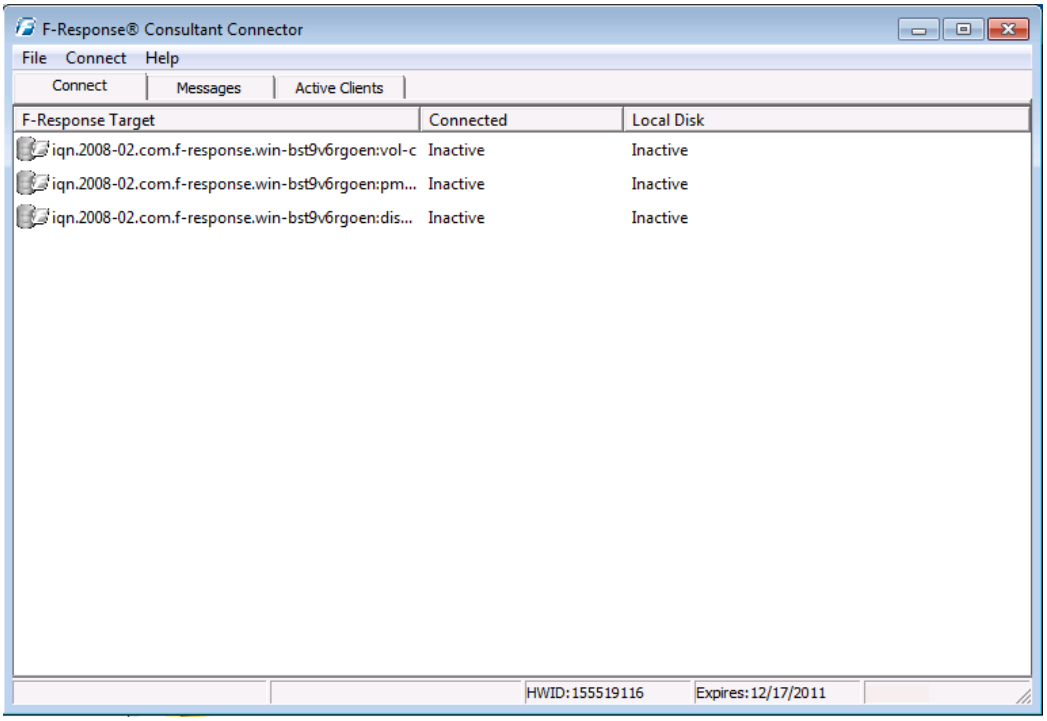
Select one or more targets and select Connect -> Login to F-Response Disk to authenticate to and access the remote device.



Following a successful login, the Target icon will indicate connected, and the Local disk column will show the locally connected disk that maps to the remote device.



To logoff of the F-Response Target, select the connected Target and select Connect -> Logout of F-Response Disk.

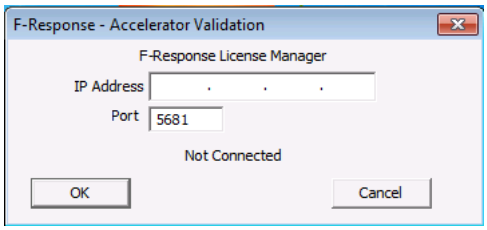


Once logoff operation completes the icon will indicate disconnected and the Local Disk column will indicate Inactive.

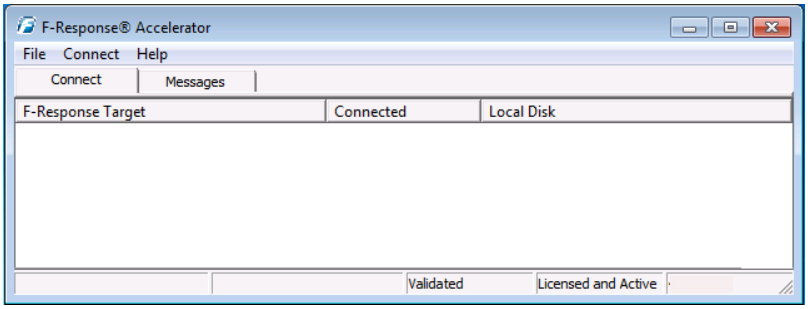
F-Response Accelerator (Consultant, Consultant + Covert, and Enterprise Only)

The F-Response Accelerator is a secondary connection utility provided to Consultant and Enterprise license holders. Essentially the Accelerator removes the need to navigate the somewhat difficult Microsoft iSCSI Initiator to connect to F-Response targets from machines that do not currently have an F-Response license dongle inserted in them.

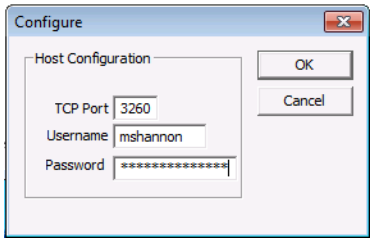
By using the F-Response Accelerator a customer can create connections from many F-Response Accelerator machines to many F-Response targets.



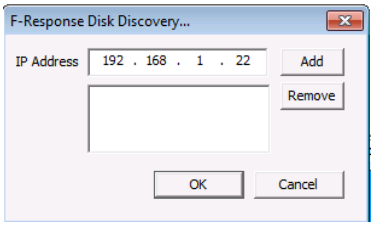
Upon starting the F-Response Accelerator you will be prompted to input the IP and Port of the F-Response License Manager in order to validate your license and begin using Accelerator



The F-Response Accelerator main window



Start by selecting File->Configure to input your F-Response username, password, and tcp port

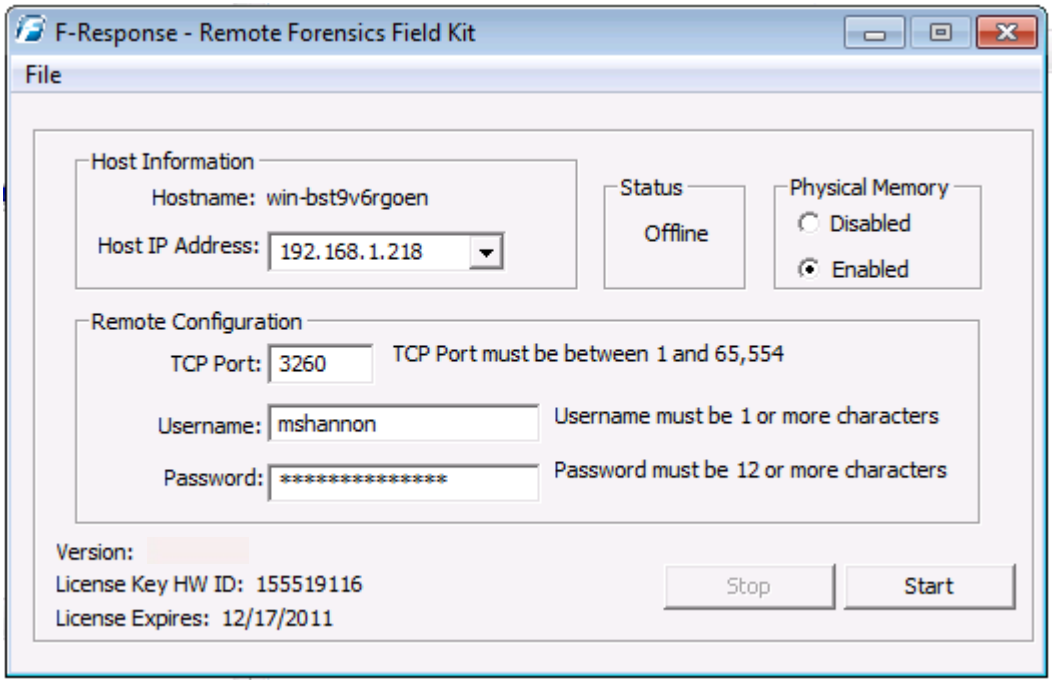


To locate F-Response Targets and connect to them start by using the Connect->Find F-Response Disks, this will open a dialog where you can input the target machine IP addresses.

Field Kit Edition

F-Response Field Kit Edition – Using F-Response Field Kit Edition for Windows

- **Step 1**
  - To use the F-Response Field Kit, insert a valid F-Response FOB key into a USB port of the computer *to be analyzed*. Make the F-Response FK Target code available to the local machine (via USB, network share, CD, et al) and execute the F-Response FK Target code. The below user interface will appear.



F-Response User Interface, configured for use. (See Appendix A for field information detail)

- **Step 2**
  - Select an IP Address from the "Host IP Address" drop-down arrow to bind the F-Response Target code to a local IP address currently in use by the computer. In this case we have chosen 192.168.1.6.
- **Step 3**
  - Select the TCP Port, in this instance we chose to keep the default '3260'.
- **Step 4**
  - Enter in a username and password value. These values will be used later to authenticate the network connection to this computer.
- **Step 5**
  - Press the "Start" button to start listening for incoming connections.

This completes F-Response preparation for this machine. Remember – **you will need the four entries selected in the User Interface above in order to establish the connection to access this computer's drives over the network.** Refer to the next section on using the Microsoft iSCSI Initiator to complete the connection and access the local machine's physical drives from remote.

F-Response Field Kit Edition – Using F-Response Field Kit Edition for Unix (Linux, Apple OS X)

```
[root@nsx mshannon]# ./f-response-fk-lin -h
F-Response Field Kit (Linux),(Version 5.0.0)
Usage:
 -h                      This help page.
 -u <username>           Username, must be eight(8) characters.
 -p <password>           Password, must be fourteen(14) characters.
 -i <port>               iSCSI port, optional, default is 3260.
 -a <path/to/device>     Assign additional devices, comma separated, ex. "-a
/dev/md0".
Examples:

To use F-Response Field Kit (Linux Edition):
f-response-fk-lin -u jsmith01 -p password123456
```

The F-Response Field Kit Edition for Apple OS X and Linux is installed and available in the C:\Program Files\F-Response\F-Response Field Kit Edition\ folder. The executable name will indicate which version is appropriate for your target platform.

F-Response Field Kit Edition for Linux – f-response-fk-lin

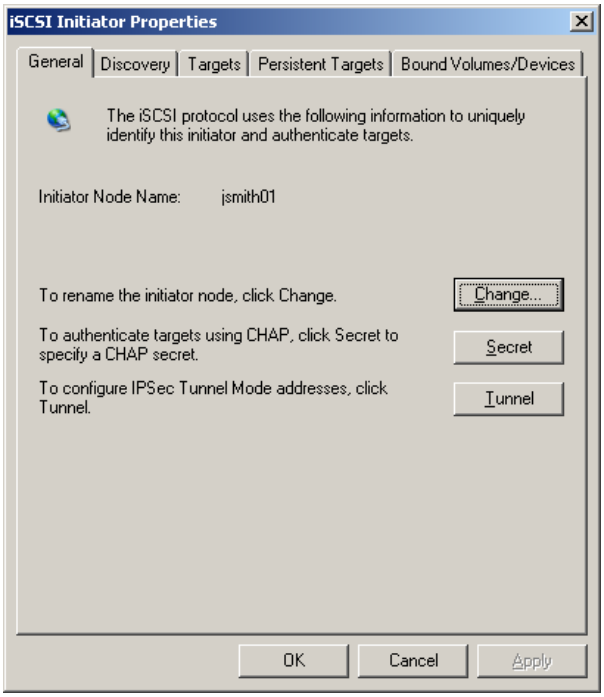
F-Response Field Kit Edition for Apple OSX (10.4, 10.5, 10.6 Intel) – f-response-fk-osx

Example Usage:

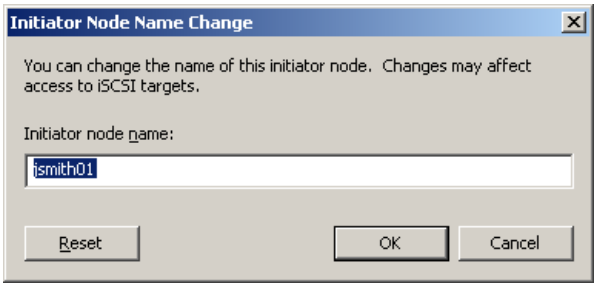
Scenario #1 – F-Response License Manager Server on 192.168.1.6, Port 5681.

```
sudo ./f-response-fk-lin -u mshannon -p mshannon123456 -i 3260
```

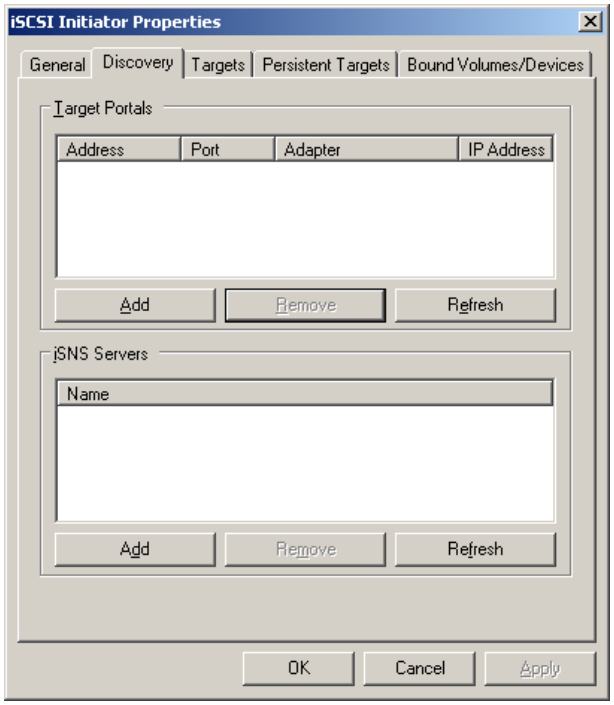
F-Response Field Kit Edition – Connecting to an F-Response Target



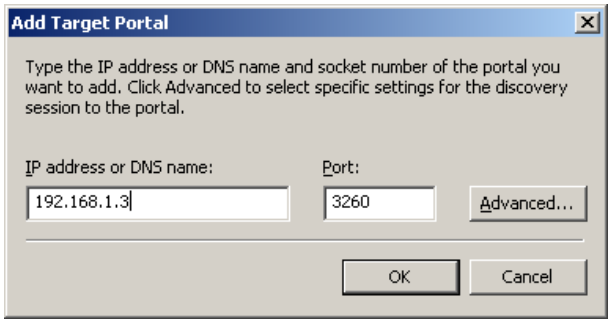
This is the Microsoft iSCSI Initiator console. First select "Change…" to rename your initiator node.



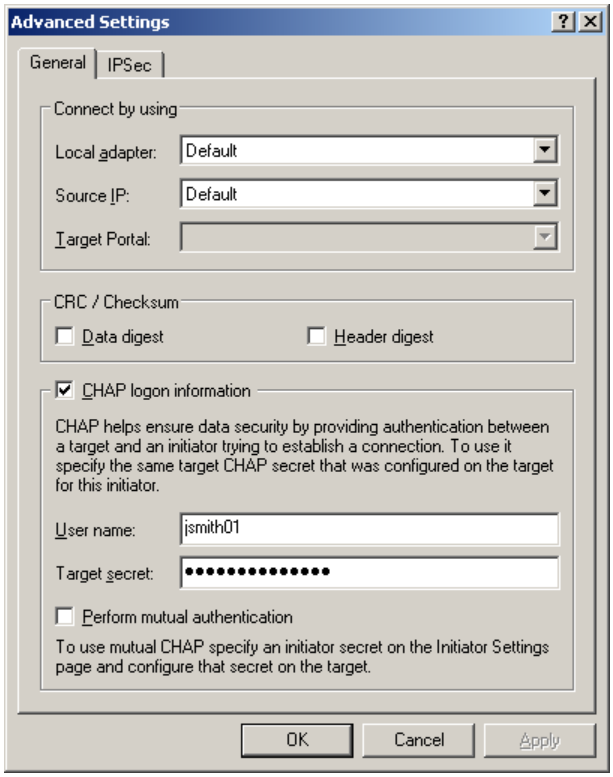
Set this value to whatever value was inputted in the F-Response Field Kit user interface username field. Select OK.



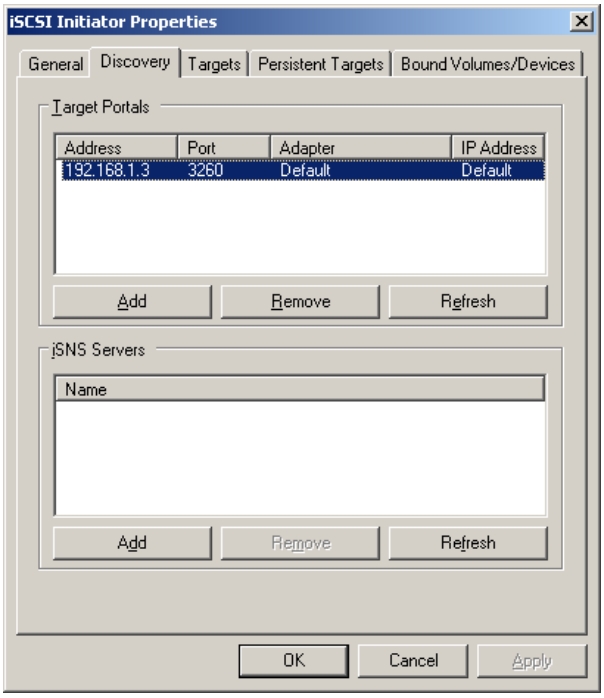
Now you must add the Target Portal. Select the Add button on the Discovery tab.


Add Target Portal
Type the IP address or DNS name and socket number of the portal you want to add. Click Advanced to select specific settings for the discovery session to the portal.
IP address or DNS name:
Port:
192.168.1.3
3260
Advanced...
OK
Cancel

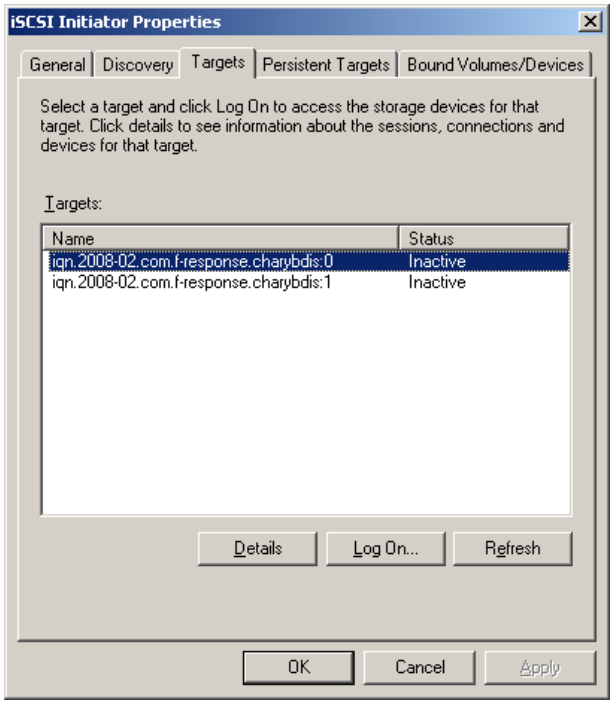
Input the IP Address and TCP port of the remote F-Response Field Kit computer. These values must match the ones entered in the F-Response Field Kit user interface. Once this is complete select the "Advanced…" button.


Advanced Settings
General
IPSec
Connect by using
Local adapter:
Default
Source IP:
Default
Target Portal:
CRC / Checksum
Data digest
Header digest
CHAP logon information
CHAP helps ensure data security by providing authentication between a target and an initiator trying to establish a connection. To use it specify the same target CHAP secret that was configured on the target for this initiator.
User name:
jsmith01
Target secret:
Perform mutual authentication
To use mutual CHAP specify an initiator secret on the Initiator Settings page and configure that secret on the target.
OK
Cancel
Apply

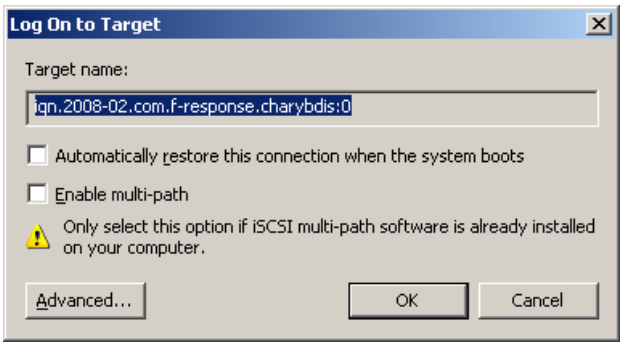
Check the box for "CHAP logon information" and enter the Username and Password previously entered into the F-Response Field Kit user interface. Select OK.



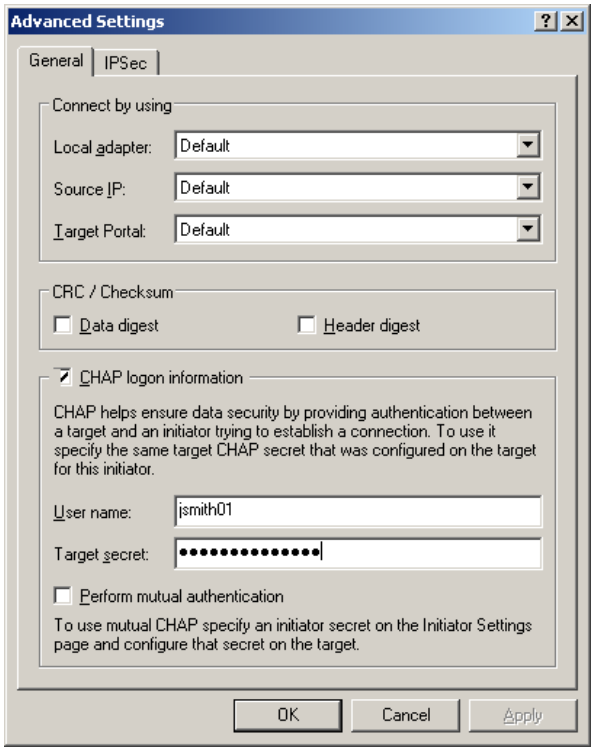
The machine running your Target code now appears in the Target Portals listing under the Discovery tab. Once this is complete provided all inputs are valid, select the Targets Tab.



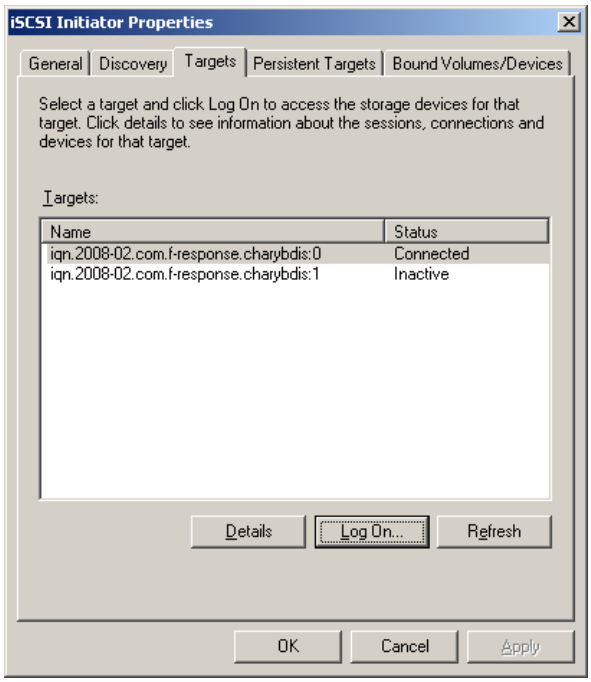
The Targets tab will show a valid target for each physical device on the F-Response Field Kit Target computer. In the above instance there are two valid physical disks on the remote computer. In addition, you will note the network name of the computer, in this case "charybdis", which is included in the target name to differentiate multiple targets. Select a target to connect to and select "Log On".



Now, select the "Advanced…" button.

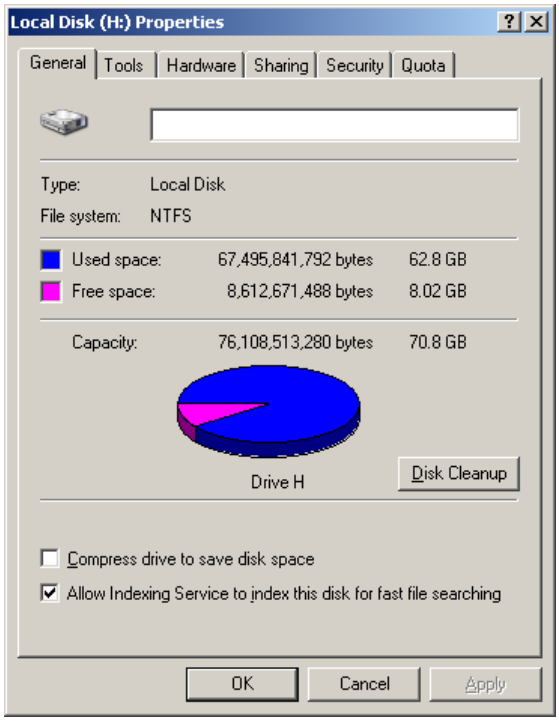

Advanced Settings
General
IPSec
Connect by using
Local adapter:
Default
Source IP:
Default
Target Portal:
Default
CRC / Checksum
Data digest
Header digest
CHAP logon information
CHAP helps ensure data security by providing authentication between a target and an initiator trying to establish a connection. To use it specify the same target CHAP secret that was configured on the target for this initiator.
User name:
jsmith01
Target secret:
Perform mutual authentication
To use mutual CHAP specify an initiator secret on the Initiator Settings page and configure that secret on the target.
OK
Cancel
Apply

Under Advanced Settings, check the CHAP logon information check box and input the Username and Password defined on the F-Response Field Kit user interface. Select Ok to complete.



Provided the Username and Password information was entered correctly and any necessary firewall modifications have been performed, you should see Status "Connected". At this point the

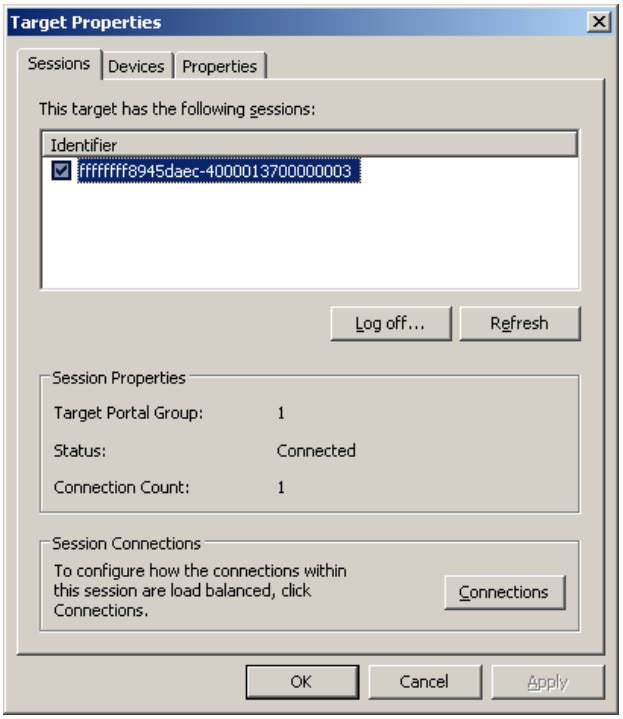
remote Physical Disk is considered a local Physical Disk on your analysis workstation. You can connect to additional targets if desired using the same process.



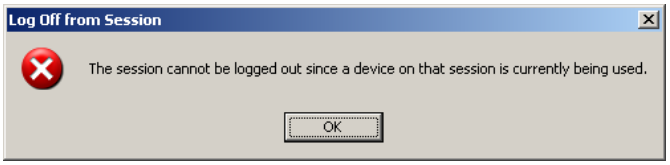
As noted earlier, the remote Physical Disk has been attached by the iSCSI Initiator and operating system, which in this instance is presented as Local Disk (H:). This drive is also accessible as a raw Physical Disk using any Computer Forensics or eDiscovery application. You can use Device Manager to verify that the remote devices appear as local physical disks.

F-Response Field Kit Edition – Disconnecting from an F-Response Target

When you are finished reviewing the disk, close all open disk access programs (e.g. Folders open, software reviewing the disk, etc). Select the connected target from the iSCSI Initiator console and select "Details". Check the box for "Identifier" and select "Log off…".

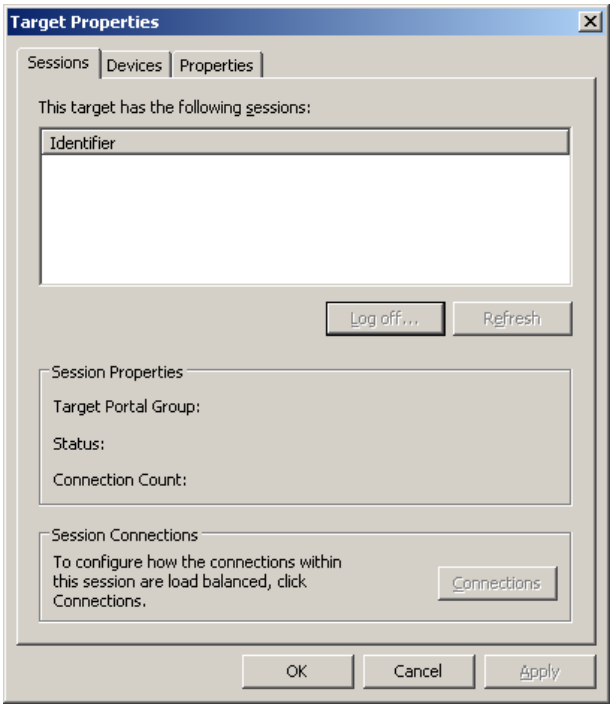


WARNING: If the disk is still in use (i.e. Folders open, software reviewing the disk, etc) Windows will not release the disk and will provide the following warning message.



Be sure to close all open disk access before selecting "Log off…"

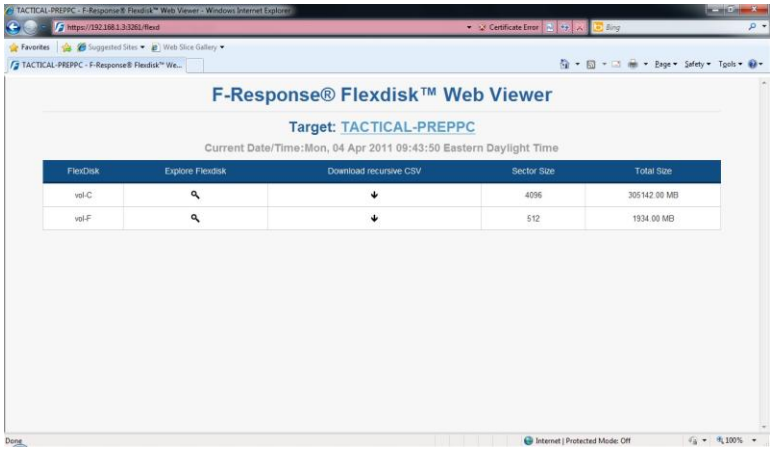
If the Initiator still does not permit the session to be logged off, you can force the session to close by selecting the stubborn Target under the "Discovery" tab, and selecting "Remove".



Once successfully logged off, the Session Identifier should be removed.

You can continue working – adding and deleting sessions, as needed – or if you are finished working, you may now close the Microsoft iSCSI initiator and stop F-Response Field Kit on the Target computer.

F-Response Flexdisk™



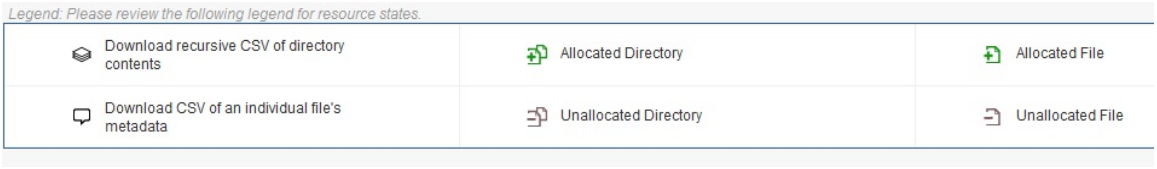
F-Response Flexdisk™ Web Viewer

What is a F-Response Flexdisk™?

The F-Response Flexdisk® (Patented) is a web based disk access and representation tool. The Flexdisk™ uses standard web technologies (HTTPS/REST[6]) to provide direct access to the remote target machines Logical and Physical targets in both raw and logical format. The Flexdisk™ can be accessed and used from any modern web browser and also exposes a feature rich and extensible application programming interface (API) accessible from any system capable of making and interpreting web queries and JSON[7].

How do I access and use a F-Response Flexdisk™?

Using the F-Response Flexdisk™ is as easy as working with a web browser. The Flexdisk™ web viewer interface contains multiple icons as well as a clearly defined legend to cover their usage and meaning. A sample of that legend appears below:


Legend: Please review the following legend for resource states.
Download recursive CSV of directory contents
Allocated Directory
Allocated File
Download CSV of an individual file's metadata
Unallocated Directory
Unallocated File

In addition to using the provided web viewer, the F-Response Flexdisk™ provides a rich and capable web services API that can be used to build mobile and web based applications that leverage F-Response Flexdisk™ provided content. More information of using the Flexdisk™ API is

[6] REST or Representational State Transfer is a web services development model that uses simple HTTP verbs such as GET and POST.
[7] JSON or Javascript Object Notation is a data formatting style considered smaller and easier to manipulate when compared to XML.

available in the Flexdisk™ API document available on the Downloads page of the F-Response Website.

Frequently Asked Questions

1. **Q)** Can multiple initiators connect to a single F-Response target machine?
2. **Q)** Do I change any data on the target computer by using F-Response?
3. **Q)** I am connected via F-Response. I navigated to a file on the remote computer, hit delete, and it appears to be gone. Did I really delete the file?
4. **Q)** I have a personal firewall running on my computers. Do I need to change firewall settings to use F-Response?
5. **Q)** I have a remote user that accidentally deleted a file. Can I use F-Response to recover deleted files?
6. **Q)** Is the F-Response iSCSI connection encrypted?
7. **Q)** Does F-Response work as an agent?
8. **Q)** Can I deploy F-Response to Linux or Other Operating Systems (OS's)?
9. **Q)** When I attempt to deploy F-Response using the FEMC I cannot, even though I have valid credentials?
10. **Q)** I established an F-Response connection, tried to view the remote "Documents and Settings" folder and received a message that I don't have permission to view that folder. Why don't I have access?
11. **Q)** What port does the F-Response EMC management console use to deploy and manage the F-Response Service?
12. **Q)** Where does the F-Response EMC management console "install" or place the F-Response Enterprise executable and configuration file?
13. **Q)** What port does the F-Response EMC management console use to deploy and manage the F-Response Service?

1. **Q)** Can multiple initiators connect to a single F-Response target machine?
   A) While the F-Response target code is running, any iSCSI initiator with access to the listening port can connect to the machine; provided, of course, that the proper authentication credentials are provided.

2. **Q)** Do I change any data on the target computer by using F-Response?
   A) Once the F-Response Target code is executed and the network connection is established, the practitioner conducting the analysis cannot edit or alter data on the machine under inspection via the F-Response connection. Executing or starting the F-Response service does, of course, effect some change to the target computer, but the changes are about as minimal as they can be for analysis that is being conducted on a live machine.

3. **Q)** I am connected via F-Response. I navigated to a file on the remote computer, hit delete, and it appears to be gone. Did I really delete the file?
   A) No, you didn't delete the file. You cannot delete files, alter Meta data, or effect any other changes on the machine under inspection using F-Response. What you did do was fool your analysis machine into "believing" that the file is deleted and thus your analysis machine is no longer presenting the file to you as available.

4. **Q)** I have a personal firewall running on my computers. Do I need to change firewall settings to use F-Response?

A) Possibly, F-Response does create temporary exceptions in the Windows Firewall during execution. Furthermore these exceptions are removed when the application exits. However, if you are using a firewall other than the Microsoft Windows Firewall, you may need to set an exception. F-Response machines must be able to send and receive on port 3260 (this default is changeable) and if using the Enterprise or Consultant Edition, also port 5681 (this default is changeable). We recommend disabling the firewall for the duration of the session during ad hoc usage (e.g. temporary consultant use at a third party site), and tuning the firewall configurations to allow F-Response connectivity for planned enterprise deployment.

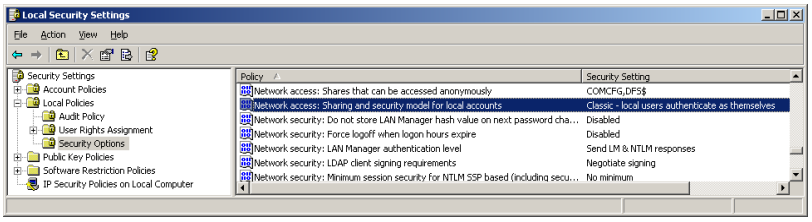
5. **Q)** I have a remote user that accidentally deleted a file. Can I use F-Response to recover deleted files?
   A) F-Response will enable you to use your recovery tool of choice to recover the file(s) to a location other than the target machine. You cannot restore the file directly to the target machine via F-Response because you do not have write capability on that machine, but you can recover the file and make it available to the user via email, network share, etc.

6. **Q)** Is the F-Response iSCSI connection encrypted?
   A) By default, no. However AES 256 bit Encryption is available in F-Response Enterprise edition. Alternatively, there are native methods to accomplish this, if needed. E.g. using Microsoft IPSec policy manager you can create a configuration to enforce an IPSec policy in your enterprise governing ports 3260, or whatever port you have elected to use with F-Response. This could be used to force F-Response to be used over an IPSec tunnel, and thus allow you to have the F-Response service start automatically with each boot. If F-Response is being used over the Internet and corporate policy dictates encryption over public networks, then the existing corporate VPN capability should satisfy the encryption policy.

7. **Q)** Does F-Response work as an agent?
   A) No. It does not collect or store any data on the machine under inspection. It does not report to a management server. It does not have an inherent analysis or reporting capability.

8. **Q)** Can I deploy F-Response to Linux or Other Operating Systems (OS's)?
   A) Yes, we have support for 7+ Non Windows Operating systems. See the platforms supported section of this document for further details.

9. **Q)** When I attempt to deploy F-Response using the FEMC I cannot, even though I have valid credentials?
   A) Your target machine is most likely a Windows XP machine not running in "Classic" mode for credential authentication. This is typically the case when attempting to connect to XP machines not part of a Windows Domain. To switch the target machine to Classic you must open the Local Security Policy Administration Tool under Control Panel, Administrative Tools. You will then select Local Policies->Security Options and change the value of "Network Access: Sharing and Security Model for Local Accounts" to "Classic – Local Users authenticate as themselves". This is only necessary in when using the FEMC to deploy F-Response to XP or greater computers not part of a Windows Domain.


Local Security Settings
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Public Key Policies
Software Restriction Policies
IP Security Policies on Local Computer
Policy
Security Setting
Network access: Shares that can be accessed anonymously
COMCFG,DFS$
Network access: Sharing and security model for local accounts
Classic - local users authenticate as themselves
Network security: Do not store LAN Manager hash value on next password cha...
Disabled
Network security: Force logoff when logon hours expire
Disabled
Network security: LAN Manager authentication level
Send LM & NTLM responses
Network security: LDAP client signing requirements
Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secu...
No minimum

If the target machine is a Windows 7, Vista, or newer Windows OS and not joined to a Domain (ie. Workgroup Member) then a key will need to be added to the registry of the target machine. You can manually create and add this key to the registry by following these steps:

To create your registry key, copy the following information into Notepad:
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"LocalAccountTokenFilterPolicy"=dword:00000001

Save this file as LocalAccountTokenFilterPolicy.reg, and then copy it to your target machine. Double click this file on the target machine to populate the registry with this key.

To remove follow the same steps as above this time with the following information:
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"LocalAccountTokenFilterPolicy"=dword:00000000

10. **Q)** I established an F-Response connection, tried to view the remote "Documents and Settings" folder and received a message that I don't have permission to view that folder. Why don't I have access?
    A) You have the access with the right tools. You probably used Windows Explorer or an equivalent tool that is subject to the file permission settings for those folders. If you use a forensics tool that can take advantage of your raw drive access, then you won't have this issue.

11. **Q)** What port does the F-Response EMC management console use to deploy and manage the F-Response Service?
    A) The F-Response EMC uses Microsoft File and Printer Sharing services for remote administration and deployment, TCP Port 445.

12. **Q)** Where does the F-Response EMC management console "install" or place the F-Response Enterprise executable and configuration file?
    A) The F-Response EMC places the executable and configuration file in the C:\Windows|WINNT\System32|SysWow64 folder depending on Windows version.

13. **Q)** What port does the F-Response EMC management console use to deploy and manage the F-Response Service?
    A) The F-Response EMC uses Microsoft File and Printer Sharing services for remote administration and deployment, TCP Port 445.

Support

Didn't find what you're looking for in the manual? Many of our customers find that our growing selection of brief tutorial videos offers the information to meet their immediate needs:

https://www.f-response.com/support/videos

We take pride in providing prompt attention to your support needs, and will support your F-Response product for the period of your license term. F-Response support can be reached via

Email: support@f-response.com
Website (Chat Support): https://www.f-response.com

Software and documentation updates will be made available for download to registered users on the F-Response web site. E-mail support is available to licensed software users. We typically respond to your queries within 1 business day of receiving your request.

Mission Guides

What are Mission Guides?

F-Response Mission Guides were designed to simplify the process of using F-Response software in new and unfamiliar scenarios. Mission guides offer a possible solution to your task, working with you each step of the way through instruction that is direct and to the point. Much smaller than a manual, Mission Guides give you the exact information you need to get you connected and underway as fast as possible.

Mission Guides are simple, straight forward, 4-6 page PDF documents that cover all the steps necessary to accomplish a specific "Mission" with F-Response. All Mission Guides are available at https://www.f-response.com/support/missionguides under the "Support" link at the top of every page. A selection of the Mission Guides available at the time this document was developed is available below:

- F-Response Enterprise Edition
  - Connect to a remote Linux target(s) disk using F-Response Enterprise Edition
  - Connect to a remote Apple target(s) disk using F-Response Enterprise Edition
  - Connect to a remote Windows target(s) disk using F-Response Enterprise Edition
  - Connect to the F-Response Boot CDROM using F-Response Enterprise Edition
- F-Response Consultant Edition
  - Connect to a remote Linux target(s) disk using F-Response Consultant Edition
  - Connect to a remote Apple target(s) disk using F-Response Consultant Edition
  - Connect to a remote Windows target(s) disk using F-Response Consultant Edition
  - Connect to the F-Response Boot CDROM using F-Response Consultant Edition
- F-Response Field Kit Edition
  - Connect to the F-Response Boot CDROM using F-Response Field Kit Edition
- F-Response TACTICAL
  - Connect to the F-Response Boot CDROM using F-Response TACTICAL

Software Revision History

The following list identifies changes made to the F-Response software:

F-Response 5.0.1 contains the following new features and enhancements:
Changes affecting Enterprise, Consultant + Covert, Consultant Edition, and TACTICAL

- Update to the F-Response Cloud Connector, including:
    - Dropbox
        - Updates to correct Modified Metadata, prior release month values were off by one, ie (February would be identified as January, etc).
- Updates to the F-Response Enterprise Management Console to detect remote machines with non-standard root Windows System path.
- Updates to the F-Response HP_UX 11i executable to include detection of logical volumes.
- Updates to the F-Response Flexdisk Technology (Linux, Windows, and OSX)
    - JSON output now contains additional entries for alternate data streams with NTFS
    - JSON output includes higher resolution time values in addition to Unix timestamp values where possible.

F-Response 5.0.0 contains the following new features and enhancements:
Changes affecting Enterprise, Consultant + Covert, and Consultant Edition

- Update to the F-Response Cloud Connector, including improved handling of non-printable characters, and support for the following newly added Cloud Storage environments:
    - Google Drive
        - Includes Google Drive and Google Apps for Business Drive access.
    - Dropbox
    - Microsoft Skydrive
- Updates to the F-Response Email Connector, including improved handling of IMAP throttling, newly added support for Office 365 using native Microsoft Exchange Web Services, a new configure options dialog for selectable options, and support for accessing Gmail Calendar exports.
- Updates to the Database Connector including improved handling of potentially corrupt Sharepoint instance data.
- Additional error details for all Connector Suite products, as well as additional error details for non-standard iSCSI interactions.
- Corrections to the F-Response COM Objects to handle Active Clients logic.
- Updates to the F-Response COM Object Script samples.
- Updated version of the F-Response executable for HPUX, corrected potential incorrect drive size report.

Changes affecting the Enterprise and Consultant + Covert version of F-Response

- Updates to the F-Response Enterprise Management Console or Covert Console to better handle unix systems with non-standard shell interaction. This net result should be improved deployment capability for non-windows systems.

F-Response 4.0.06 contains the following new features and enhancements:
Changes affecting Enterprise, Consultant + Covert, and Consultant Edition

- New F-Response Database Object Connector, providing access to embedded file database objects. Supports Microsoft Sharepoint Databases on Microsoft SQL Server.
- New F-Response Email Connector, providing access to remote IMAP email as a local read-only volume. Includes support for Gmail, Yahoo! Mail, and any generic IMAP based (SSL or Non-SSL) email server.

- Windows 8 Support for all F-Response Connector series products.
- F-Response License Update check now occurs silently when dongle is within ten days of expiration.
- Corrected the License Manager Monitor to better handle rare timeout issues when starting the License Manager Service.

Changes affecting the Consultant version of F-Response

- General usability updates for the F-Response Consultant Connector, context menu corrections, etc.

Changes affecting all versions of F-Response

- Updates to all versions of F-Response to better support target machines with a large number of disk devices.

F-Response 4.0.05 contains the following new features and enhancements:

Changes affecting Enterprise and Consultant + Covert Edition

- F-Response Cloud Connector has been updated to use a new caching model which greatly improves speed and performance.
- F-Response Enterprise COM Object has been improved to better detect and deploy to newer versions of Linux, including recent Ubuntu releases (12.04, 12.10).
- F-Response FreeBSD executable now included for 64bit FreeBSD on Intel.
- Minor performance updates to the F-Response Enterprise Management Console and Covert Console to improve speed and platform support.
- F-Response Enterprise Management Console and Covert Console now able better able to detect and deploy to legacy Windows computers.
- F-Response Enterprise COM Object for x64 Windows is now included with the standard installation (on x64 examiner machines).
- F-Response Enterprise Management Console, Cover Console, and F-Response Accelerator now remove legacy iSCSI target portals on logout to reduce confusion.
- F-Response Enterprise Management Console and Covert Console now able to assign a Service Description to the F-Response Enterprise Service [Optional].
- Direct Connect option in the both management consoles has been multi-threaded, resulting in a faster and more robust user experience.
- F-Response Cloud Connector (Enterprise version only) no longer requires local dongle, support license manager operation (similar to Accelerator).

Changes affecting Consultant Edition

- F-Response Consultant Connector now removes legacy iSCSI target portals on logout to reduce confusion.
- F-Response Consultant COM object for x64 Windows now included in the standard installation (on x64 examiner machines).
- F-Response FreeBSD executable now included for 64bit FreeBSD on Intel.

Changes affecting all versions of F-Response

- New F-Response Dongle Updater has been added to Enterprise, Consultant+Covert, Consultant, and Field Kit. This new updater uses a new "upt2" file format and removes the requirement to download a separate dongle updater from the F-Response website when renewing or upgrading your license.
- Windows 8 Support for all F-Response Examiner products (FEMC, FCC, etc) has been added.
- F-Response target executable for Windows now better able to handle physical memory on Windows 2000 systems.

F-Response 4.0.04.1 contains the following new features and enhancements:
Changes affecting Enterprise Edition and Consultant + Covert Edition

- F-Response Cloud Connector now supports Windows Azure Blob Storage.

Changes affecting all versions of F-Response

- Improved handling of non-standard mount points in Linux.
- Improved Physical Memory access stability based on further input from the Volatility Project.

F-Response 4.0.04 contains the following new features and enhancements:
Changes affecting Enterprise and Consultant + Covert Edition

- New F-Response Cloud Connector providing direct read-only access to Cloud Storage Environments, including Amazon S3, Rackspace Cloud Files, HP Public Cloud, and any v1 Openstack implementation.
- F-Response Enterprise Management Console now correctly detects Apple OSX 10.8 target computers and deploys the appropriate software.
- F-Response Consultant + Covert is now better able to detect Windows machines even if they are running SSH/SFTP services.
- Improved handling of deployment to remote Windows machines with non-standard root directories and paths.
- New Export MSI… option exports the F-Response target executable and configuration file along with all necessary settings to a simple Microsoft Installer which can be easily deployed to target machines using 3rd party deployment tools.

Changes affecting all versions of F-Response

- F-Response Apple OSX executables now signed with registered Apple Developer certificate.
- F-Response Linux and Apple OSX executables now able to better detect non-standard device paths and mount points and automatically add these as available targets.
- Thanks to assistance from AAron Walters, Michael Ligh, and the Volatility Project, F-Response Physical Memory access now has greatly improved stability in large memory environments.

F-Response 4.0.03 contains the following new features and enhancements:
Changes affecting Enterprise and Consultant + Covert Edition

- F-Response Enterprise now includes support for 64bit Linux platforms.
- F-Response Enterprise Management Console now correctly detects Apple OSX 10.7 target computers and deploys the appropriate software.
- F-Response Flexdisk updated with minor API corrections based on user feedback.
- F-Response Enterprise Service Uninstall issue addressed, removed potential "service marked for deletion" issue.
- Updated Spanish language text as per user input.

Changes affecting Consultant Edition

- F-Response Consultant Edition updated to address potential "service marked for deletion" issue.
- F-Response Flexdisk updated with minor API corrections based on user feedback.
- F-Response Consultant Edition now includes support for 64bit Linux platforms.

Changes affecting Field Kit Edition

- F-Response Field Kit Edition updated to address potential "service marked for deletion" issue.

F-Response 4.0.02.1 contains the following new features and enhancements:
Changes affecting Enterprise Edition

- Enterprise Encryption is now updated to properly handle logical volumes and +2TB devices.

Changes affecting Consultant Edition

- Improved handling of > 2TB disks for non-Windows platforms.

Changes affecting Field Kit Edition

- Improved handling of > 2TB disks for non-Windows platforms.

F-Response 4.0.02 contains the following new features and enhancements:
Changes affecting Enterprise Edition

- F-Response Enterprise now provides the option to encrypt all read actions directed to remote targets.
    - Encryption is AES using 256 bit keys.
    - Encryption is optional and can be enabled or disabled.
    - Encryption requires Windows Vista or better on the Examiner machine, ie the machine running either the FEMC or the F-Response Accelerator.
- F-Response Flexdisk updated with new programmable API.
    - Flexdisk™ now has programmable API using simple RESTful web methods and JSON text encoding. More information on the Flexdisk™ API is available in the API document on the Downloads page of the F-Response website.
- F-Response Flexdisk™ for Linux now autodetects more mount points and logical volumes.
- Updates to the F-Response Enterprise COM Scripting object to support Flexdisk configuration options.
- Improved handling of > 2TB disks for non-Windows platforms.
- F-Response Enterprise for AIX and SCO now more accurately locates and presents physical devices.

Changes affecting Consultant Edition

- F-Response Flexdisk updated with new programmable API.
    - Flexdisk™ now has programmable API using simple RESTful web methods and JSON text encoding. More information on the Flexdisk™ API is available in the API document on the Downloads page of the F-Response website.
- F-Response Flexdisk™ for Linux now autodetects more mount points and logical volumes.
- Improved handling of > 2TB disks for non-Windows platforms.
- F-Response Consultant for AIX and SCO now more accurately locates and presents physical devices.

Changes affecting Field Kit Edition

- Improved handling of > 2TB disks for non-Windows platforms.
    - lerator.
- F-Response Flexdisk updated with new programmable API.
    - Flexdisk™ now has programmable API using simple RESTful web methods and JSON text encoding. More information on the Flexdisk™ API is available in the API document on the Downloads page of the F-Response website.
- F-Response Flexdisk™ for Linux now autodetects more mount points and logical volumes.
- Updates to the F-Response Enterprise COM Scripting object to support Flexdisk configuration options.
- Improved handling of > 2TB disks for non-Windows platforms.
- F-Response Enterprise for AIX and SCO now more accurately locates and presents physical devices.

F-Response 4.0.01 contains the following new features and enhancements:
Changes affecting Enterprise Edition

- F-Response Enterprise Management Console (FEMC) now provides rapid deployments options which condense the standard deployment steps.
    - Install/Start F-Response
        - Will install, start, and issue discovery against a remote F-Response target.
    - Stop/Remove F-Response
        - Will stop and remove F-Response from a remote target.
- Added an Active Clients menu to allow for the selective enabling or disabling of the standard continuous polling mechanism used to update active clients.
- Added an "Export" option to the Deployment Options dialog to make the manual deployment process easier. Export button will allow the user to save off a copy of the ini file and selected executable prepared for manual deployment.
- Added the new patent pending F-Response Flexdisk™ capabilities to F-Response Enterprise Windows, Linux, and OSX (Apple) targets.
- Added the new F-Response Accelerator to allow many-to-many connectivity for F-Response Enterprise and Consultant customers.

Changes affecting Consultant Edition

- Modified the F-Response Consultant Connector (FCC) to improve responsiveness.
- Added the new patent pending F-Response Flexdisk™ capabilities to F-Response Consultant Windows, Linux, and OSX (Apple) targets.
- Added the new F-Response Accelerator to allow many-to-many connectivity for F-Response Enterprise and Consultant customers.

F-Response 3.09.09 contains the following new features and enhancements:
Changes affecting All Versions

- F-Response (All Versions) now provides support for accessing physical disks > 2TB, theoretical limit of 8+ Zettabytes.
- Modifications to correct authentication/login/logout issues when connecting from Linux (open-iscsi).

Changes affecting Enterprise Edition

- Adjustments to the F-Response Enterprise Management Console(FEMC) to support different IP Address configurations.
- Added logic to handle F-Response Deployment to remote target machines using a non-standard root drive.
- F-Response License Manager Monitor (LMM) now opens the dialog automatically on first load.
- Addressed an issue with correctly handling alternate port selection from the command line or via configure options.
- Icon display corrected for FEMC Direct Connect for Windows targets.
- F-Response License Manager now automatically populates Validation Port and IP in Configure Options.
- F-Response Enterprise now provides target support for the following new platforms:
    - Android (ARM)
    - NetGear NAS (SPARC)

Changes affecting Consultant Edition

- Added auto IP detection to the F-Response Consultant Connector (FCC) to enable automatic configuration of the F-Response License Manager (LM) IP Address.
- F-Response License Manager Monitor (LMM) now opens the dialog automatically on first load.
- F-Response License Manager now automatically populates Validation Port and IP in Configure Options.
- F-Response Consultant now provides target support for the following new platforms:
    - Android (ARM)
    - NetGear NAS (SPARC)

F-Response 3.09.08/3.09.08.1 contains the following new features and enhancements:

Changes affecting All Versions

- F-Response (All Windows Versions) now provides support for accessing physical disks > 2TB, theoretical limit of 8+ Zettabytes.
- Corrected an issue with the 32bit Physical Memory access driver that caused stability issues in certain situations.

Changes affecting Enterprise Edition 3.09.08.1

- The F-Response Enterprise Scripting Object (FEMCCTRL) 3.09.08.1 has been updated to include improved error handling and revised methods. Contains updated FEMCCTRL COM Object corrected to handle Credential creation issue and modified Configure File path. Sample scripts for using the object have been provided for Visual Basic Script, Perl, Python, and C#.
- F-Response Enterprise now provides explicit audit logs for Login/Logout/Failed Login/Start/Stop operations on remote targets. Audit logs are found in the Application Event Logs of the F-Response License Manager.
- F-Response Enterprise is now fully Terminal Services/Remote Desktop aware allowing multiple users on a single machine to run the F-Response Enterprise Management Console (FEMC) simultaneously.
- F-Response Enterprise now provides target support for OpenSolaris.

Changes affecting Consultant Edition

- The F-Response Consultant Connector Scripting Object (FCCCTRL) has been released with methods and properties to automate connecting to deployed F-Response Consultant Edition Targets. Sample scripts for using the object have been provided for Visual Basic Script, Perl, and Python.
- F-Response Consultant now provides target support for OpenSolaris.

F-Response 3.09.07 contains the following new features and enhancements:

Changes affecting All Versions

- F-Response (All Versions) now provides support for physical memory access under both 32bit and 64bit Windows environments.
- Added a F-Response Linux (< 60 Meg) Boot CDROM that provides access to F-Response FK, CE, EE, and TACTICAL. Boot CDROM is available to all licensed customers.
- Corrected an issue where disk read errors on the target side could cause an iSCSI disconnect that was not automatically reconnected.

Changes affecting Enterprise Edition

- The F-Response Enterprise Scripting Object (FEMCCTRL) has been updated to include improved error handling, additional objects, properties, and methods. Sample

scripts for using the object have been provided for Visual Basic Script, Perl, Python, and C#.
- Corrected an issue where the FEMC Unix Deployment options may be incorrectly loaded/presented.
- Added additional platform checking options to handle Linux and Apple OS builds returning non-typical chipset types and processor configurations.

F-Response 3.09.06 contains the following new features and enhancements:
Changes affecting Enterprise Edition
- F-Response Enterprise now provides full deployment via the Enterprise Management Console (FEMC) to all supported platforms.
- FEMC now has both a Credentials and Options Configure panel, including platform specific configuration options and Unix based credentials.
- The Messages panel now indicates the presence of new messages with the (!) notation.
- The Custom Scan dialog now presents the last custom scan performed.
- Microsoft iSCSI Initiator issues related to listing targets on 64bit Windows platforms have been resolved.
- The FEMC now determines the License Manager IP Address automatically if it is running and correctly updates the configuration information without user interaction.

Changes affecting Consultant Edition
- F-Response Consultant now offers the option for configuring to bind to all IP addresses (both in autoconfigure generation and on the CE client GUI).
- The Messages panel now indicates the presence of new messages with the (!) notation.
- Microsoft iSCSI Initiator issues related to listing targets on 64bit Windows platforms have been resolved.

F-Response 3.09.05 contains the following new features and enhancements to the Consultant and Enterprise Edition
- F-Response is now a Microsoft Winqual validated and approved Windows 7 Compatible Application
- F-Response provides additional support for the following platforms:
- HP Unix (HP_UX11iv2, HP_UX11iv3) on Itanium
- FreeBSD 7 on Intel/i386
- F-Response now addresses the "Unable to logoff of disk" issue in Windows Vista, 2008, and Windows 7 both 32 and 64bit.

F-Response 3.09.04 contains multiple enhancements and bug fixes for all versions of F-Response, including:
Changes affecting all versions
- Passive Hibernation/Suspend prevention. F-Response (FK, CE, EE) when running under Windows will prevent the passive hibernation/suspend of the MUI. Active suspend/hibernation actions (such as closing the laptop screen, etc) will still be performed

Changes affecting F-Response Consultant Edition (Windows)
- F-Response Consultant Connector now provides a “Clear Messages” option that removes all text from the Messages Panel.
- F-Response Consultant Edition (f-response-ce.exe) now has the ability to completely hide the dialog window on the remote machine with a simple key sequence, (ALT-CTRL-F12). This sequence will hide the GUI and restore the GUI.

Changes affecting F-Response Enterprise Edition (Windows)

- Issue in password generation for command line usage of F-Response Enterprise corrected.
- F-Response Enterprise Management Console now provides a "Clear Messages" option that removes all text from the Messages Panel.
- The F-Response Enterprise installation package now includes a partial implementation of the F-Response Enterprise Management Console in a language neutral fully scriptable COM object. This object will allow a technical user of F-Response Enterprise to script actions typically initiated manually in the FEMC. For a sample script see the C:\Program Files\F-Response\ folder.

F-Response 3.09.03 New Features (All versions)

- Username and Password length are now more flexible. Username must be 1+ ANSI characters, Password must be 12-16 ANSI characters, in keeping in line with specifications.

New Features Consultant and Enterprise Edition

- Minor updates to both management consoles reflecting the changed password length criteria. Also additional error/informational messages in the "Messages" panel when issuing a Discovery Request, Login, or Logoff.
- Management Consoles will automatically enable iSCSI services on Vista+ operating systems when started (if they are not already on).

F-Response 3.09.02 New Features (All versions)

- All F-Response software (Windows) has been translated into German, Spanish, and Simplified Chinese.
- Username and Password length are now more flexible. Username must be 1+ ANSI characters, Password must be 12+ ANSI characters.
- All Windows based F-Response software now includes UAC support for proper prompting under Vista, 2008, and Windows 7.

New Features Consultant and Enterprise Edition

- Minor updates to the F-Response License Manager, including better dongle stability, improved error codes, additional support for the Windows Event Log.
- Support for Sun Solaris 8, 9, 10 on SPARC.
- Support for IBM AIX 5.3 on Power5 and Power6.

F-Response 3.09.1 New Features (Consultant and Enterprise Editions only)

New Features Consultant Edition

- New F-Response License Manager, small, faster, easier to work with, replaces the NetUniKey.
- Updated F-Response Consultant Connector
- Right click context menus throughout
- Support for removing Connect Tab target entries

New Features Enterprise Edition

- New F-Response License Manager, small, faster, easier to work with.
- Updated F-Response Enterprise Management Console
- Right click context menus throughout
- Support for removing Connect Tab target entries
- Additional Custom Scan option for scanning by comma separated list of machine names or IP addresses
- Direct Connect dialog user interaction streamlined

F-Response 3.09 contains multiple enhancements and bug fixes for all versions of F-Response, including:

Changes affecting all versions

- Logical Volume and Physical Memory(32bit Windows Only) support, now F-Response locates and provides access to physical disks, logical volumes, and physical memory.
- Automatic Firewall exceptions (Windows Firewall Only), F-Response now creates and removes firewall exceptions automatically.
- New platform support, Linux (glibc >= 2.3.5) and Apple OSX 10.4,10.5

Changes affecting F-Response Consultant Edition

- Newly released F-Response Consultant Connector streamlines the process of connecting and disconnecting from remote F-Response Consultant Edition clients.
- Newly released F-Response License Manager (Monitor, Service) replaces the NetUniKey server. Provides a more streamlined interface and improved platform support options.

Changes affecting F-Response Enterprise Edition

- Newly released F-Response Enterprise Management Console streamlines the complete lifecycle of F-Response Enterprise, deploy, connect, disconnect, and remove F-Response Enterprise clients from a single interface.
- Newly released F-Response License Manager (Monitor, Service) replaces the NetUniKey server. Provides a more streamlined interface and improved platform support options.

Changes affecting F-Response Field Kit Edition

- Support for Linux (glibc 2.3.5+) and Apple OS X 10.4, 10.5 Intel only.

F-Response 1.18 contains multiple enhancements and bug fixes for all versions of F-Response, including:

Changes affecting all versions

- Improved handling of foreign language versions of Windows.
- Added support for non-standard Windows Computer Names.
- Improved on-load drive probing.
- Official support for the Open-iSCSI Linux Initiator.
- Un-Official support for the GlobalSAN iSCSI Initiator for Apple OSX.
- Improved thread management performance.
- Updated Version information to 1.18.

Changes affecting F-Response Field Kit Edition

- Graphical user interface now includes the F-Response license expiration date.

Changes affecting F-Response Consultant Edition

- Graphical user interface now includes the F-Response license expiration date.
- Autoconfigure option for F-Response Consultant edition added, allows F-Response Consultant Edition to be run from CD or to be provided to IT staff with no repeated configuration needed.

F-Response 1.17 contains multiple enhancements and bug fixes for all versions of F-Response, including:

Changes affecting all versions

- Modified disk capacity return value in accordance with SCSI parameters.
- Corrected issue relating to STOP ERROR for Microsoft iSCSI Initiator in select circumstances.
- Updated Version information to 1.17.

Changes affecting F-Response Field Kit Edition

- Modified License controls to allow more leeway when dealing with inaccurate system clocks.

Changes affecting F-Response Consultant Edition

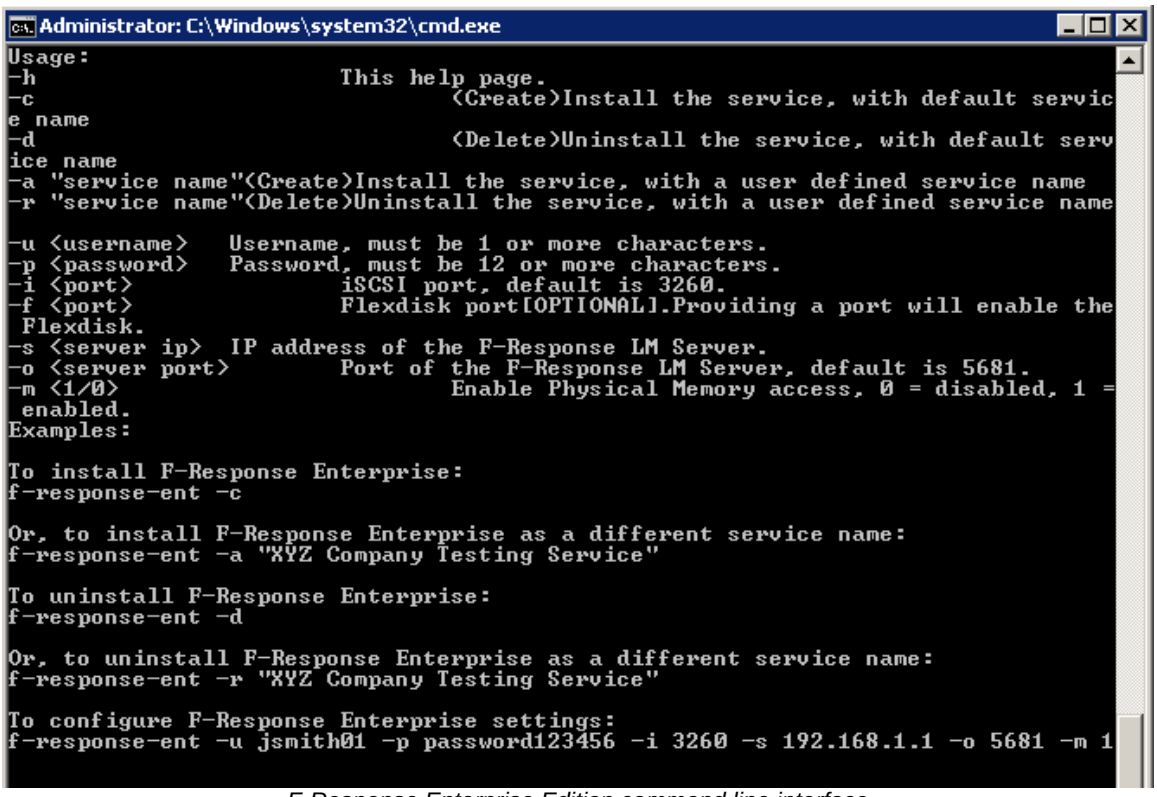
- Improved performance of IP validation look-up process.

Changes affecting F-Response Enterprise Edition

- Modified iSCSI Target IP selection based on IP target for Discovery.
- Added command line options (-a, -r) to add and remove F-Response Enterprise Service using user defined name.

Appendix A – Overview of the F-Response Enterprise Edition Windows Command Line Interface

This appendix provides details regarding the command line options for installing, uninstalling, and configuring F-Response Enterprise on each target machine. The help text is shown in the following screen capture:


Administrator: C:\Windows\system32\cmd.exe
Usage:
-h This help page.
-c (Create)Install the service, with default servic
e name
-d (Delete)Uninstall the service, with default serv
ice name
-a "service name"(Create)Install the service, with a user defined service name
-r "service name"(Delete)Uninstall the service, with a user defined service name
-u <username> Username, must be 1 or more characters.
-p <password> Password, must be 12 or more characters.
-i <port> iSCSI port, default is 3260.
-f <port> Flexdisk port[OPTIONAL].Providing a port will enable the
Flexdisk.
-s <server ip> IP address of the F-Response LM Server.
-o <server port> Port of the F-Response LM Server, default is 5681.
-m <1/0> Enable Physical Memory access, 0 = disabled, 1 =
enabled.
Examples:
To install F-Response Enterprise:
f-response-ent -c
Or, to install F-Response Enterprise as a different service name:
f-response-ent -a "XYZ Company Testing Service"
To uninstall F-Response Enterprise:
f-response-ent -d
Or, to uninstall F-Response Enterprise as a different service name:
f-response-ent -r "XYZ Company Testing Service"
To configure F-Response Enterprise settings:
f-response-ent -u jsmith01 -p password123456 -i 3260 -s 192.168.1.1 -o 5681 -m 1

F-Response Enterprise Edition command line interface

F-Response Enterprise edition is a GUI-less Windows Service version of the F-Response Target Code. It was designed for ease of administration and distribution to remote targets. The screen capture above provides the f-response-ent.exe help page, including several examples.

The following help text details the command line options for installing, uninstalling, and configuring F-Response Enterprise on each target machine.

Installing & Uninstalling F-Response Enterprise:

- -c {Create}, -d {Delete}
  - These options are mutually exclusive. They either install (-c) or uninstall (-d) the service on the local target computer with the default service name "F-Response Enterprise Service". Note: You can change the name of the F-Response Enterprise executable file to anything you like prior to installation (e.g. you may rename "f-response-ent.exe" to "xyz_tester.exe"). You may also place the F-

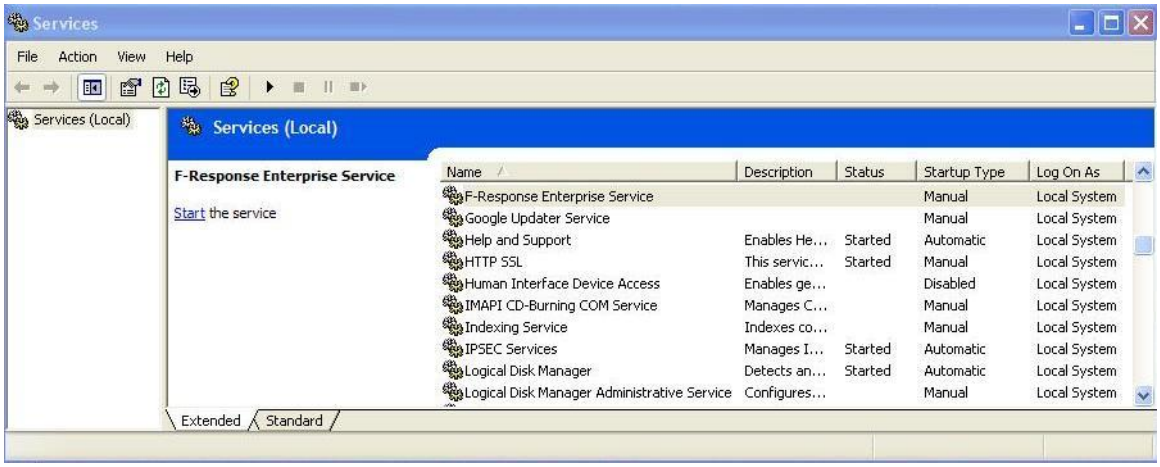
Response Enterprise executable file anywhere you like prior to installation (e.g. \WINDOWS\system32).

- -a ("user defined service name"), -r ("user defined service name")
  - These options are mutually exclusive. They either install (-a) or uninstall (-r) the service on the local computer *with a user defined service name*. Note: You can change the name of the F-Response Enterprise executable file to anything you like prior to installation (e.g. you may rename "f-response-ent.exe" to "xyz_tester.exe"). You may also place the F-Response Enterprise executable file anywhere you like prior to installation (e.g. \WINDOWS\system32).

Configuring F-Response Enterprise:

- -s (Server IP), -o (Server Port)
  - Since the Enterprise Edition of F-Response allows the F-Response FOB to be physically remote from the computer to be analyzed, the Enterprise Edition software must be configured with parameters identifying the network address (Server IP) and port number (Server Port) of the computer to which the F-Response FOB is connected, and which is running the NetUniKey Server (often the IP Address of an Enterprise Investigations Server).
  - Completing a successful configuration creates a "NetUniKey.ini" file. For successful execution of F-Response Enterprise, both the F-Response Enterprise executable ("f-response-ent.exe" by default) and the "NetUniKey.ini" file must be located in the same folder on the target computer.

- -u (username), -p (password), -i (iSCSI Port), -f (Flexdisk™ Port)
  - These options set the username, password, and iSCSI port that will be used for remote connectivity by the iSCSI initiator. If the Flexdisk™ port is not specified it will not be enabled.


Services
File Action View Help
Services (Local)
Services (Local)
F-Response Enterprise Service
Start the service
Name Description Status Startup Type Log On As
F-Response Enterprise Service Manual Local System
Google Updater Service Manual Local System
Help and Support Enables He... Started Automatic Local System
HTTP SSL This servic... Started Manual Local System
Human Interface Device Access Enables ge... Disabled Local System
IMAPI CD-Burning COM Service Manages C... Manual Local System
Indexing Service Indexes co... Manual Local System
IPSEC Services Manages I... Started Automatic Local System
Logical Disk Manager Detects an... Started Automatic Local System
Logical Disk Manager Administrative Service Configures... Manual Local System
Extended Standard

F-Response Enterprise Edition Service Management Console interface

The F-Response Enterprise service is controlled via the Microsoft Management Console for Services. By default the service is installed in the Manual position, such that it may be started during an investigation and stopped when no longer needed. Once installed and configured, the service need only be "started" each time it is to be used. The default service name "F-Response

Enterprise Service" can be replaced with a user defined service name during installation with the "-a" option.

Appendix B – Overview of the F-Response Enterprise Edition Unix Command Line Interface

```
F-Response Consultant/Enterprise (<PLATFORM>),(Version 3.09.06)
Usage:
  -h                              This help page.
  -a </path/to/devices>           Path to additional devices (Comma
separated, ex /dev/md0,/dev/md1)
  -S <F-ResponseLM IP>            IP Address of F-Response LM Server
  -P <F-ResponseLM Port>          TCP Port of F-Response LM Server, optional,
defaults to 5681
  -u <username>                   F-Response username, must be 8 characters
  -p <password>                   F-Response password, must be 14 characters
  -i <iSCSI Port>                 iSCSI Port, optional, defaults to 3260
  -c <path/to/fresponse.ini>      Optional autoconfigure path, if used no
other commandline options are required

F-Response Consultant/Enteprise Edition can either be run directly from the
commandline (using the various arguments indicated above, or it can be run
with the -c <path/to/fresponse.ini> option provided the path points to a
valid fresponse.ini file. See the F-Response Consultant Connector
autoconfigure option to generate a valid "fresponse.ini"
```

The F-Response Enterprise Edition for Linux, Apple OS X, HP_UX, AIX, Sun Solaris, and FreeBSD is installed and available in the C:\Program Files\F-Response\F-Response Enterprise Edition\ folder. The executable name will indicate which version is appropriate for your target platform.

- F-Response Enterprise Edition for Linux – f-response-ce-e-lin
- F-Response Enterprise Edition for Apple OSX (10.3, 10.4, 10.5 Intel & PPC) – f-response-ce-e-osx
- F-Response Enterprise Edition for Sun Solaris – f-response-ce-e-sun
- F-Response Enterprise Edition for IBM AIX (Power) – f-response-ce-e-aix-p5
- F-Response Enterprise Edition for HP Unix – f-response-ce-e-hpux
- F-Response Enterprise Edition for FreeBSD – f-response-ce-e-fbsd
- F-Response Enterprise Edition for SCO Unix – f-response-ce-e-sco

Example Usage:

Scenario #1 – F-Response License Manager Server on 192.168.1.6, Port 5681.

```
sudo ./f-response-ce-e-lin -S 192.168.1.6 -P 5681 -u mshannon -p
mshannon123456 -i 3260
```

Scenario #2 – F-Response Autconfigure file "fresponse.ini" created using F-Response Consultant Connector

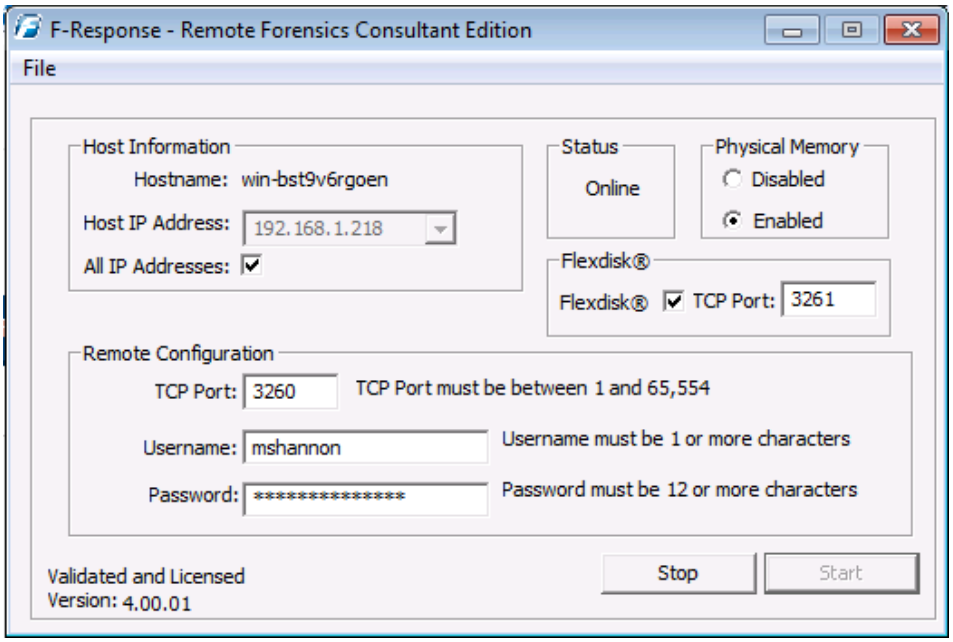
```
sudo ./f-response-ce-e-lin -c ./fresponse.ini
```

Scenario #3 – F-Response Autconfigure file "f-response-ent.exe.ini" created by the F-Response FEMC Console following a successful Configuration (C:\Program Files\F-Response\F-Response Enterprise\f-response-ent.exe.ini)

```
sudo ./f-response-ce-e-lin -c ./fresponse.ini
```

Appendix C – Overview of the F-Response Consultant User Interface

This appendix provides an explanation of the fields presented by the F-Response Consultant User Interface, which is presented upon execution of the F-Response Consultant Edition User Interface Target code on the computer *to be analyzed*.



F-Response Consultant Edition User Interface

An explanation of the fields presented by the F-Response Consultant Edition Target code is as follows:

- **Host Information**
  - Hostname
    - This is the Machine Name or Host Name of the local machine upon which the F-Response Target code has been run.
  - Host IP Address
    - This is a drop down listing of the IP addresses configured on this local Target machine. If there are multiple addresses present you should select the one most readily accessible as this will be the address you connect to from your remote analysis machine via the Initiator.

- **Remote Configuration**
  - TCP Port
    - This is the TCP port your remote or Initiator computer will use to connect to the local machine. The iSCSI default is 3260; however you may assign another available TCP port if desired.
  - Username
    - The iSCSI protocol requires a username for the remote Initiator computer connection. The username selected must be one or more

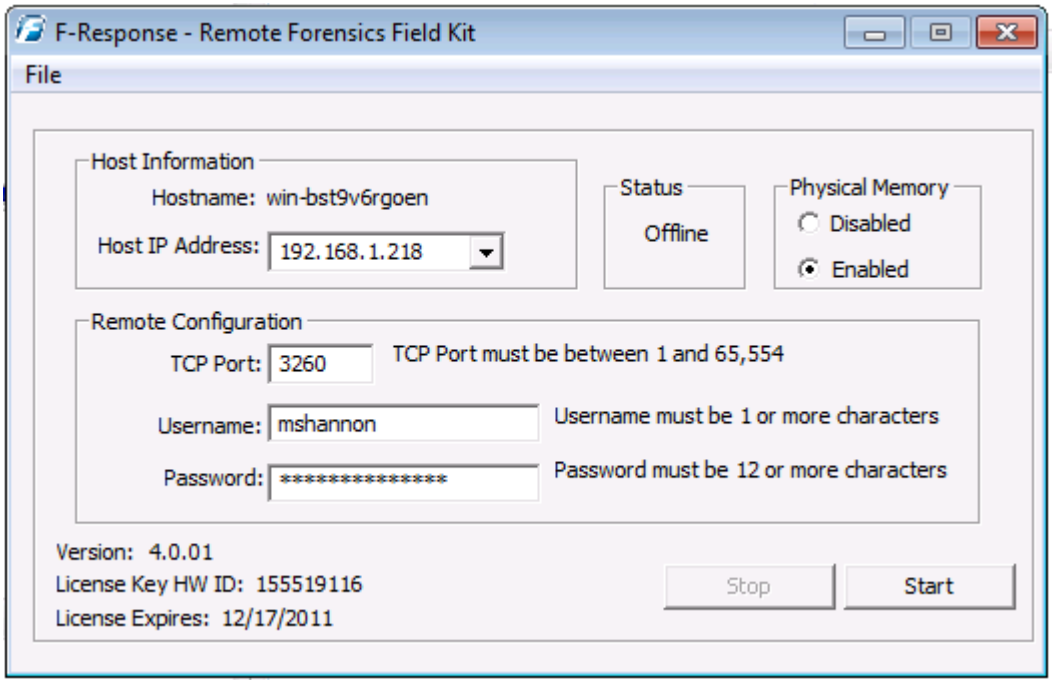
characters in length. This username will be used on the remote Initiator computer to access the local or Target machine's hard drives.

- Password
  - The iSCSI protocol requires a password for the remote Initiator computer connection. The password selected must be 12 or more characters in length. This password will be used on the remote Initiator computer to access the local or Target machine's hard drives.

- **Version**
  - This is the version of F-Response Consultant Edition target code that you are using; in this case Version 4.00.01

Appendix D – Overview of the F-Response Field Kit User Interface

This appendix provides an explanation of the fields presented by the F-Response Field Kit User Interface, which is presented upon execution of the F-Response Field Kit User Interface Target code on the computer *to be analyzed*.



F-Response Field Kit Edition User Interface

An explanation of the fields presented by the F-Response Field Kit Edition Target code is as follows:

- **Host Information**
  - Hostname
    - This is the Machine Name or Host Name of the local machine upon which the F-Response Target code has been run.
  - Host IP Address
    - This is a drop down listing of the IP addresses configured on this local Target machine. If there are multiple addresses present you should select the one most readily accessible as this will be the address you connect to from your remote analysis machine via the Initiator.

- **Remote Configuration**
  - TCP Port
    - This is the TCP port your remote or Initiator computer will use to connect to the local machine. The iSCSI default is 3260, however you may assign another available TCP port if desired.
  - Username
    - The iSCSI protocol requires a username for the remote Initiator computer connection. The username selected must be one or more

characters in length. This username will be used on the remote Initiator computer to access the local or Target machine's hard drives.

- Password
  - The iSCSI protocol requires a password for the remote Initiator computer connection. The password selected must be exactly 12 or more characters in length. This password will be used on the remote Initiator computer to access the local or Target machine's hard drives.

- **Version**
  - This is the version of F-Response Field Kit Edition target code that you are using; in this case Version 4.00.01.

- **License Key HW ID**
  - This is the Hardware ID of your F-Response FOB. This ID number is required when upgrading or renewing your F-Response software license.

- **License Expires**
  - This is the expiration date of the license encoded to your F-Response FOB. This number will appear in "red" when your F-Response software license is due to expire within 30 days.

Appendix E – Understanding Unix Credentials

F-Response uses Unix Credentials and the Secure Shell service (SSH/SFTP) to access remote non-Windows based machines. In order to utilize this service you'll want to familiarize yourself with Unix credentials.

User accounts and Credentials

For our purposes there are two different user accounts we can use to gain sufficient access to a target non-Windows based machine, a general user account, and "root".

In the Unix world "root" is the superuser or Administrator. As you can imagine using the superuser or "root" account can be dangerous therefore most system administrators allow general user account to perform actions requiring "root" level permission through one of two options, su and sudo.

Assume User (su)

Using "su" a general user account can assume superuser privileges for a limited period of time. The user will require the "root" or superuser password to gain these privileges, and once the "su" action is complete the user will effectively be able to perform any and all actions as "root" or superuser. It is sometimes easiest to think of this process much like Windows User Account Controls (Windows UAC) in Microsoft Windows Vista and 7, you are asked to use "su" as an extra step in an effort to make you cognitive of the powerful capabilities your account now possesses.

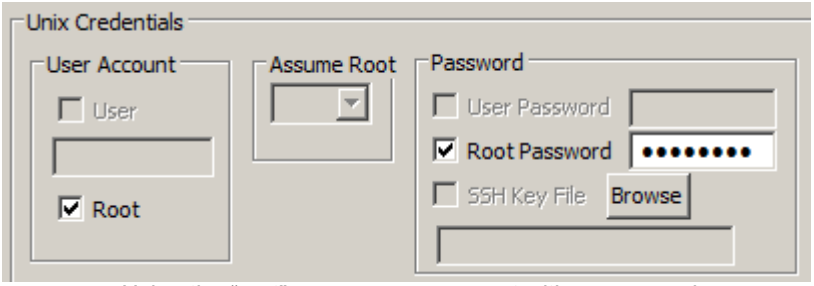
Superuser do (sudo)

Using "sudo" a general user is allowed to execute a specific command with superuser privileges. In this instance the user need only enter their user password when prompted. Again, much like the Windows UAC process, you are asked to use sudo as an extra step in an effort to make you aware of the actions your account is temporarily capable of.

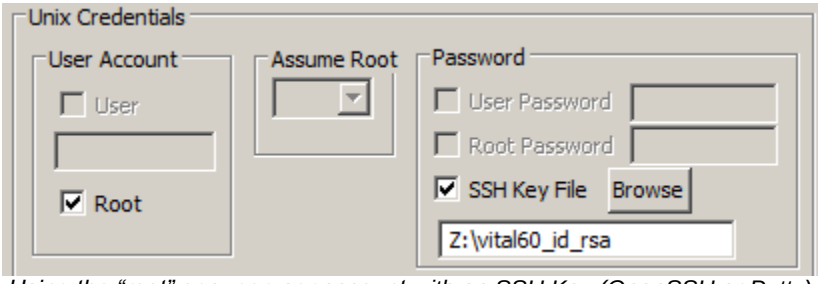
SSH Keys

Many system administrators prefer to allow remote connections only when they are attempted using a special cryptographic key file, the SSH Key File. F-Response allows you to specify a key file for access, however unless your account is the "root" or superuser account you will need to provide the appropriate password for "su" or "sudo". F-Response supports both OpenSSH and Putty SSH Key files.

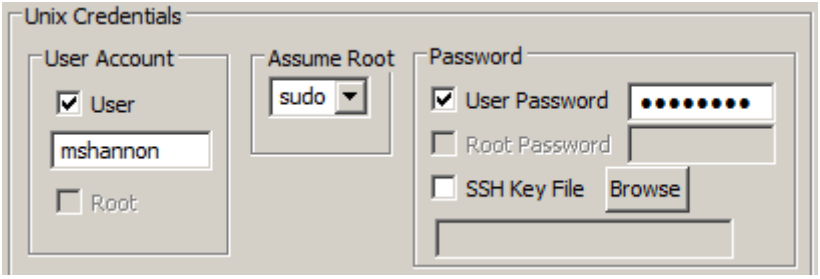
F-Response allows you to access the remote machine with any combination of user account and credential, however let's go through a few common scenarios below:



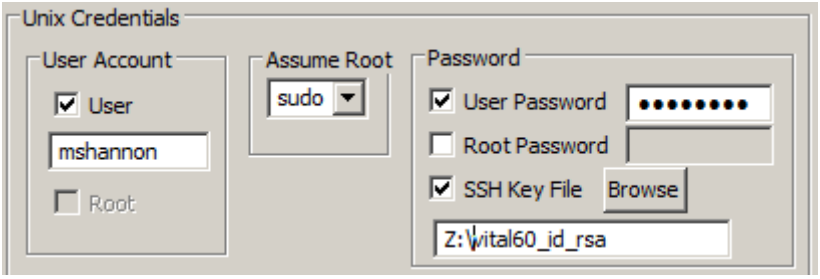
Using the "root" or superuser account with a password



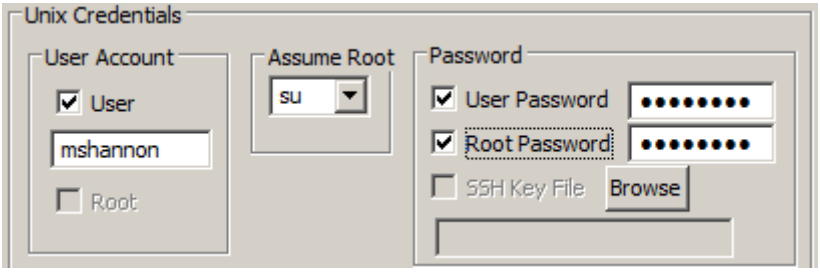
Using the "root" or superuser account with an SSH Key (OpenSSH or Putty)



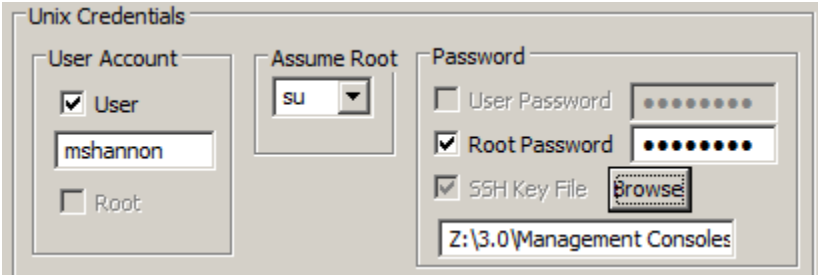
Using a general user account, sudo, and a user password for access and sudo permissions



Using a general user account, sudo, and a user password for sudo permissions plus an SSH Key for access



Using a general user account, su, and a user password for access plus the root password for su permissions



Using a general user account, su, and a SSH key for access plus the root password for su permissions

Appendix F – Software Requirements on the Target Computer

The following outlines what software, services, and credentials are required to connect to a remote target computer via the F-Response Enterprise Management Console (FEMC)

- Windows (All Versions)
  - Software
    - No additional
  - Services
    - File and Printer Sharing (Microsoft Services TCP Port 445)
  - Credentials
    - Administrator or like permission sufficient to create a LocalSystem level service
- Unix (All Versions)
  - Software
    - No additional
  - Services
    - SSH with SFTP Subsystem services available
  - Credentials
    - User account capable of assuming superuser privileges, or superuser account
- Platform Specific Notes
  - Apple
    - SSH is not enabled by default on Apple OSX, however it can be enabled via the System Preferences via the "Remote Login" Service. The exact location of this option will vary by operating system release and version.

Appendix G – F-Response Target Naming Convention

The following outlines the F-Response Target naming convention:

- All Platforms
  - iqn.2008-02.com.f-response.HOSTNAME.
- Windows
  - Physical Disk
    - …disk-X (where x is the physical disk number)
  - Logical Volume
    - …vol-X (where x is the logical volume letter)
  - Physical Memory
    - …pmem
- Non-Windows
  - Physical Disk
    - …<disk name> (platform dependent)

Appendix H -- Icon Legend

Icon	Platform	Name	Details
	None	Network Domain or Workgroup	Icon indicates a Network Domain or Workgroup, computers listed under this icon have identified themselves as being a member of the group.
	Unknown	Unknown	Icon indicates this computer platform is unknown or valid credentials could not be established, check the Messages tab for further details.
	Apple	Apple F-Response Not Installed	Icon indicates an Apple Computer, if no badge is present the Apple computer is available and does not have F-Response Installed. If a badge is present check the badge legend below for further details.
	FreeBSD	FreeBSD F-Response Not Installed	Icon indicates a FreeBSD Computer, if no badge is present the FreeBSD computer is available and does not have F-Response Installed. If a badge is present check the badge legend below for further details.
	HPUX	HP Unix F-Response Not Installed	Icon indicates a HP Unix Computer, if no badge is present the HP Unix computer is available and does not have F-Response Installed. If a badge is present check the badge legend below for further details.
	AIX	IBM AIX F-Response Not Installed	Icon indicates a IBM AIX Computer, if no badge is present the AIX computer is available and does not have F-Response Installed. If a badge is present check the badge legend below for further details.
	Linux	Linux F-Response Not Installed	Icon indicates a Linux Computer, if no badge is present the Linux computer is available and does not have F-Response Installed. If a badge is present check the badge legend below for further details.
	SCO	SCO Unix F-Response Not Installed	Icon indicates a SCO Unix Computer, if no badge is present the SCO computer is available and does not have F-Response Installed. If a badge is present check the badge legend below for further details.

	Solaris/OpenSolaris (SunOS)	Sun Solaris F-Response Not Installed	Icon indicates a Sun Solaris Computer, if no badge is present the Solaris computer is available and does not have F-Response Installed. If a badge is present check the badge legend below for further details.
	Windows	Windows F-Response Not Installed	Icon indicates a Windows Computer, if no badge is present the Windows computer is available and does not have F-Response Installed. If a badge is present check the badge legend below for further details.
GreyScale Icon(s)	All Platforms	Machine not accessible	A grayscale icon indicates the target computer is not accessible with the credentials provided.

Badges (appear over icons)

Badge	Name	Details
	F-Response Started	This badge indicates F-Response has been started on the target Computer.
	F-Response Stopped	This badge indicates F-Response has been stopped on the target Computer.

Appendix I – Master Software License Agreement

AGILE RISK MANAGEMENT LLC MASTER SOFTWARE LICENSE AGREEMENT
TERMS AND CONDITIONS

1. Scope of Agreement; Definitions. This Agreement covers the license and permitted use of the Agile Risk Management LLC ("Agile") F-Response Software. Unless otherwise defined in this section, the capitalized terms used in this Agreement shall be defined in the context in which they are used. The following terms shall have the following meanings:

1.1. "Agile Software" or "Software" means any and all versions of Agile's F-Response software.

1.2. "Customer" means the person or entity identified on the invoice and only such person or entity, Customer shall not mean any assigns, heirs, or related persons or entities or claimed third-party beneficiaries of the Customer.

1.3. "Documentation" means Agile release notes or other similar instructions in hard copy or machine readable form supplied by Agile to Customer that describes the functionality of the Agile Software

1.4. "License Term" means the term of the applicable license as specified on an invoice or as set forth in this Agreement.

2. Grant of Software License.

2.1. Enterprise License. Subject to the terms and conditions of this Agreement only, Agile grants Customer a non-exclusive, non-transferable license to install the Agile Software and to use the Agile Software during the License Term, in object code form only.

2.2. Third Party Software. Customer acknowledges that the Agile Software may include or require the use of software programs created by third parties, and the Customer acknowledges that its use of such third party software programs shall be governed exclusively by the third party's applicable license agreement.

3. Software License Restrictions.

3.1. No Reverse Engineering; Other Restrictions. Customer shall not, directly or indirectly: (i) sell, license, sublicense, lease, redistribute or transfer any Agile Software; (ii) modify, translate, reverse engineer, decompile, disassemble, create derivative works based on, or distribute any Agile Software; (iii) rent or lease any rights in any Agile Software in any form to any entity; (iv) remove, alter or obscure any proprietary notice, labels or marks on any Agile Software. Customer is responsible for all use of the Software and for compliance with this Agreement and any applicable third party software license agreement.

3.2. Intellectual Property. Agile retains all title, patent, copyright and other intellectual proprietary rights in, and ownership of, the Agile Software regardless of the type of access or media upon which the original or any copy may be recorded or fixed. Unless otherwise expressly stated herein, this Agreement does not transfer to Customer any title, or other ownership right or interest in any Agile Software. Customer does not acquire any rights, express or implied, other than those expressly granted in this Agreement.

4. Ordering & Fulfillment. Pricing is set forth on the F-Response website and is subject to change at any time. Each order shall be subject to Agile's reasonable acceptance. Delivery terms are FOB Agile's shipping point.

5. Payments. Customer agrees to pay amounts invoiced by Agile for the license granted under this Agreement. If any authority imposes a duty, tax or similar levy (other than taxes based on Agile's income), Customer agrees to pay, or to promptly reimburse Agile for, all such amounts. Unless otherwise indicated in an invoice, all Agile invoices are payable thirty (30) days from the date of the invoice. Agile reserves the right to charge and Customer agrees to pay Agile for every unauthorized copy or unauthorized year an amount equal to the cost per copy, per year, per computer, or per user, whichever is greater, as a late payment fee in the event Customer fails to remit payments when due or Customer otherwise violates the payment provisions of this Agreement. In addition to any other rights set forth in this Agreement, Agile may suspend performance or withhold fulfilling new Customer orders in the event Customer has failed to timely remit payment for outstanding and past due invoices.

6. Confidentiality.

6.1. Definition. "Confidential Information" means: (a) any non-public technical or business information of a party, including without limitation any information relating to a party's techniques, algorithms, software, know-how, current and future products and services, research, engineering, vulnerabilities, designs, financial information, procurement requirements, manufacturing, customer lists, business forecasts, marketing plans and information; (b) any other information of a party that is disclosed in writing and is conspicuously designated as "Confidential" at the time of

disclosure or that is disclosed orally and is identified as "Confidential" at the time of disclosure; or (c) the specific terms and conditions of this Agreement.

6.2. Exclusions. Confidential Information shall not include information which: (i) is or becomes generally known to the public through no fault or breach of this Agreement by the receiving Party; (ii) the receiving Party can demonstrate by written evidence was rightfully in the receiving Party's possession at the time of disclosure, without an obligation of confidentiality; (iii) is independently developed by the receiving Party without use of or access to the disclosing Party's Confidential Information or otherwise in breach of this Agreement; (iv) the receiving Party rightfully obtains from a third party not under a duty of confidentiality and without restriction on use or disclosure, or (v) is required to be disclosed pursuant to, or by, any applicable laws, rules, regulatory authority, court order or other legal process to do so, provided that the Receiving Party shall, promptly upon learning that such disclosure is required, give written notice of such disclosure to the Disclosing Party.

6.3. Obligations. Each Party shall maintain in confidence all Confidential Information of the disclosing Party that is delivered to the receiving Party and will not use such Confidential Information except as expressly permitted herein. Each Party will take all reasonable measures to maintain the confidentiality of such Confidential Information, but in no event less than the measures it uses to protect its own Confidential Information. Each Party will limit the disclosure of such Confidential Information to those of its employees with a bona fide need to access such Confidential Information in order to exercise its rights and obligations under this Agreement provided that all such employees are bound by a written non-disclosure agreement that contains restrictions at least as protective as those set forth herein.

6.4. Injunctive Relief. Each Party understands and agrees that the other Party will suffer irreparable harm in the event that the receiving Party of Confidential Information breaches any of its obligations under this section and that monetary damages will be inadequate to compensate the non-breaching Party. In the event of a breach or threatened breach of any of the provisions of this section, the non-breaching Party, in addition to and not in limitation of any other rights, remedies or damages available to it at law or in equity, shall be entitled to a temporary restraining order, preliminary injunction and/or permanent injunction in order to prevent or to restrain any such breach by the other Party.

7. DISCLAIMER OF WARRANTIES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AGILE AND ITS SUPPLIERS PROVIDE THE SOFTWARE AND SUPPORT SERVICES (IF ANY) AS IS AND WITH ALL FAULTS, AND HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY (IF ANY) IMPLIED WARRANTIES, DUTIES OR CONDITIONS OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF RELIABILITY OR AVAILABILITY, OF ACCURACY OR COMPLETENESS OF RESPONSES, OF RESULTS, OF WORKMANLIKE EFFORT, OF LACK OF VIRUSES, AND OF LACK OF NEGLIGENCE, ALL WITH REGARD TO THE SOFTWARE, AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT WITH REGARD TO THE SOFTWARE.

8. Limitations and Exclusions.

8.1. Limitation of Liability and Remedies. NOTWITHSTANDING ANY DAMAGES THAT YOU MIGHT INCUR FOR ANY REASON WHATSOEVER (INCLUDING, WITHOUT LIMITATION, ALL DAMAGES REFERENCED ABOVE AND ALL DIRECT OR GENERAL DAMAGES IN CONTRACT OR ANY OTHER THEORY IN LAW OR IN EQUITY), THE ENTIRE LIABILITY OF AGILE AND ANY OF ITS SUPPLIERS UNDER ANY PROVISION OF THIS AGREEMENT AND YOUR EXCLUSIVE REMEDY HEREUNDER SHALL BE LIMITED TO THE TOTAL AMOUNT PAID BY CUSTOMER FOR THE LICENSE. THE FOREGOING LIMITATIONS, EXCLUSIONS AND DISCLAIMERS SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY REMEDY FAILS ITS ESSENTIAL PURPOSE.

8.2. Exclusion of Incidental, Consequential and Certain Other Damages. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL AGILE OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), MISREPRESENTATION, STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF AGILE OR ANY SUPPLIER, AND EVEN IF AGILE OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY OR TO ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL, DAMAGES (INCLUDING WITHOUT LIMITATION, LIABILITIES RELATED TO A LOSS OF USE, PROFITS, GOODWILL OR SAVINGS OR A LOSS OR DAMAGE TO ANY SYSTEMS, RECORDS OR DATA), WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED UPON CONTRACT, WARRANTY, TORT

(INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF ADVISED IN ADVANCE OR AWARE OF THE POSSIBILITY OF ANY SUCH LOSS OR DAMAGE.

9. Verification. Agile has the right to request Customer complete a self-audit questionnaire in a form provided by Agile. If an audit reveals unlicensed use of the Agile Software, Customer agrees to promptly order and pay for licenses to permit all past and ongoing usage.

10. Support Services

10.1. Rights and Obligations. This Agreement does not obligate Agile to provide any support services or to support any software provided as part of those services. If Agile does provide support services to you, use of any such support services is governed by the Agile policies and programs described in the user manual, in online documentation, on Agile's support webpage, or in other Agile-provided materials. Any software Agile may provide you as part of support services are governed by this Agreement, unless separate terms are provided.

10.2. Consent to Use of Data. You agree that Agile and its affiliates may collect and use technical information gathered as part of the support services provided to you, if any, related to the Software. Agile may use this information solely to improve our products or to provide customized services or technologies to you and will not disclose this information in a form that personally identifies you.

11. Miscellaneous.

11.1. Legal Compliance; Restricted Rights. Each Party agrees to comply with all applicable Laws. Without limiting the foregoing, Customer agrees to comply with all U.S. export Laws and applicable export Laws of its locality (if Customer is not located in the United States), and Customer agrees not to export any Software or other materials provided by Agile without first obtaining all required authorizations or licenses. In the event the Software is provided to the United States government it is provided with only "LIMITED RIGHTS" and "RESTRICTED RIGHTS" as defined in FAR 52.227-14 if the commercial terms are deemed not to apply.

11.2. Governing Law; Severability. This Agreement (including any addendum or amendment to this Agreement which is included with the Software) are the entire agreement between you and Agile relating to the Software and the support services (if any) and they supersede all prior or contemporaneous oral or written communications, proposals and representations with respect to the Software or any other subject matter covered by this Agreement. To the extent the terms of any Agile policies or programs for support services conflict with the terms of this Agreement, the terms of this Agreement shall control. This Agreement shall be governed by the laws of the State of Florida, USA, without regard to choice-of-law provisions. You and Agile agree to submit to the personal and exclusive jurisdiction of the Florida state court located in Tampa Florida and the United States District Court for the Middle District of Florida. If any provision of this Agreement is held to be illegal or unenforceable for any reason, then such provision shall be deemed to be restated so as to be enforceable to the maximum extent permissible under law, and the remainder of this Agreement shall remain in full force and effect. Customer and Agile agree that this Agreement shall not be governed by the U.N. Convention on Contracts for the International Sale of Goods.

11.3. Notices. Any notices under this Agreement will be personally delivered or sent by certified or registered mail, return receipt requested, or by nationally recognized overnight express courier, to the address specified herein or such other address as a Party may specify in writing. Such notices will be effective upon receipt, which may be shown by confirmation of delivery.

11.4. Assignment. Customer may not assign or otherwise transfer this Agreement without the Agile's prior written consent, which consent shall not be unreasonably withheld, conditioned or delayed. This Agreement shall be binding upon and inure to the benefit of the Parties' successors and permitted assigns, if any.

11.5. Force Majeure. Neither Party shall be liable for any delay or failure due to a force majeure event and other causes beyond its reasonable control. This provision shall not apply to any of Customer's payment obligations.

11.6. Redistribution Compliance.

(a) F-Response distributes software libraries developed by The Sleuth Kit ("TSK"). The license information and source code for TSK can be found at http://www.sleuthkit.org/. If any changes have been made by Agile to the TSK libraries distributed with the F-Response software, those changes can be found online at http://www.f-response.com/TSKinfo.

(b) A portion of the F-Response Software was derived using source code provided by Intel and Alistair Crooks (NetBSD), which requires the following notice be posted herein, and which applies only to the source code. F-Response code is distributed only in binary or object code form. F-Response source code, and any revised Intel and NetBSD code contained within the F-Response source code, is not available for distribution. The name of Intel Corporation and NetBSD are not being used to endorse or promote this product, nor is the name of the author being used

to endorse or promote this product. This information is presented solely to comply with the required Intel and NetBSD license agreements which require reproduction of the following copyright notice, list of conditions and disclaimer:

Intel License Agreement
Copyright (c) 2000, Intel Corporation
All rights reserved.
- Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Intel Corporation may not be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THEPOSSIBILITY OF SUCH DAMAGE.

Copyright © 2006 Alistair Crooks. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

11.7. General. This Agreement, including its exhibits (all of which are incorporated herein), are collectively the Parties' complete agreement regarding its subject matter, superseding any prior oral or written communications. Amendments or changes to this Agreement must be in mutually executed writings to be effective. The Parties agree that, to the extent any Customer purchase or sales order contains terms or conditions that conflict with, or supplement, this Agreement, such terms and conditions shall be void and have no effect, and the provisions of this Agreement shall control. Unless otherwise expressly set forth in an exhibit that is executed by the Parties, this Agreement shall control in the event of any conflict with an exhibit. Sections 2, 3, 5, 7, 8, and 9, and all warranty disclaimers, use restrictions and provisions relating to Agile's intellectual property ownership, shall survive the termination or expiration of this Agreement. The Parties are independent contractors for all purposes under this Agreement.

Appendix J – Renewing F-Response Dongle License

Updating the F-Response Dongle (FK,CE,CE+C,EE)

Purpose

This document identifies the steps to be taken to update your F-Response USB license key FOB (FOB) in the event that you have upgraded or renewed your license.

What You Need

In order to update your FOB you will require the following:

1. The f-response_<lic#_expdate>.upt2 file you received from Customer Support after purchasing your license renewal or upgrade from the F-Response web site.

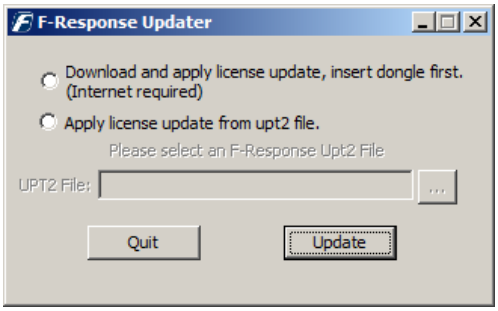
2. Your FOB, of course. Note: Upgrades and renewals are tied to a specific FOB, so be certain that you insert the proper FOB for use with the provided upt2 file.

3. A copy of the latest F-Response Updater executable file which is freely available from the F-Response Web site, or installed as part of your F-Response installation.

Step 1
Insert the FOB into an available USB port on a Windows machine.

Step 2
Execute (there is no installation process) the F-Response Updater executable file.

The following screen appears:



F-Response Updater

Step 3a
If you have Internet connectivity you can attempt to download your license file directly, select the first option and press Update.

Step 3b
If you wish to use a local upt2 file, press the second option and type in, or use the button to Browse to, the location of the upt2 file you received from Customer Support for this FOB. (Note: If you try to update the FOB for which this upt file was not intended you ll do no harm, but the process will fail.) Select Update. When the process completes in a few seconds, your license FOB has been updated, and the process is complete. Congratulations. Your FOB has now been programmed for use with your most current license.

Appendix K – Legal Notices

Legal Notice

Copyright © 2013 Agile Risk Management, LLC. All rights reserved.
This document is protected by copyright with all rights reserved.

Trademarks

F-Response is a trademark of Agile Risk Management, LLC. All other product names or logos mentioned herein are used for identification purposes only, and are the trademarks of their respective owners.

Statement of Rights

Agile Risk Management, LLC products incorporate technology that is protected by U.S. patent and other intellectual property (IP) rights owned by Agile Risk Management LLC, and other rights owners. Use of these products constitutes your legal agreement to honor Agile Risk Management, LLC's IP rights as protected by applicable laws. Reverse engineering, de-compiling, or disassembly of Agile Risk Management, LLC products is strictly prohibited.

Disclaimer

While Agile Risk Management LLC has committed its best efforts to providing accurate information in this document, we assume no responsibility for any inaccuracies that may be contained herein, and we reserve the right to make changes to this document without notice.

Patents

F-Response is covered by United States Patent Numbers: 8,171,108; 7,899,882; and other Patents Pending.